Asunto: PROCESO PARA LA AUTORIZACIÓN DE ACCESO DE LOS COMPUTADORES A OTRAS INSTALACIONES COMPUTO

1. OBJETIVO GENERAL

La División Informática establece como Política de Control de Acceso el controlar el acceso a la información, a las instalaciones de procesamiento de la información (Datacenter) y a los procesos de provisión, los cuales deberán ser controlados sobre la base de los requisitos y seguridad.

Para ello, a través de sus diferentes áreas de Operaciones, Software, Seguridad y Soporte permitirá administrar el ciclo de vida de los usuarios, desde la creación automática de las cuentas, roles y permisos necesarios hasta su inoperancia; a partir de los requerimientos reportadas por el Departamento de Recursos Humanos y/o directamente de su Jefatura directa; lo anterior para que el funcionario tenga acceso adecuado a los sistemas de información y recursos tecnológicos, validando su autenticación, autorización y auditoría.

1.1 Objetivo específico

- Identificar los requerimientos de seguridad de cada una de las aplicaciones.

- Identificar toda la información relacionada con las aplicaciones.

- Definir los perfiles de acceso de usuarios estándar, comunes a cada categoría de estaciones de trabajo.

- Administrar los derechos de acceso en un ambiente distribuido y de red, que reconozcan todos los tipos de conexiones disponibles.

- Asegurar el cumplimiento de los requisitos normativos, estatutarios, reglamentarios y contractuales, que estén orientados hacia la seguridad de la información en la Subsecretaria del Interior.

- Establecer los niveles de acceso apropiados a la información institucional, brindando y asegurando la confidencialidad, integridad y disponibilidad que requiera cada sistema y usuario.

1.2 Alcance

Esta política se aplica a todos los funcionarios, servidores públicos a honorarios y terceras partes que tengan derechos de acceso a la información que puedan afectar los activos de información de la Subsecretaría del Interior y a todas sus relaciones con terceros que impliquen el acceso a sus datos, recursos y/o a la administración y control de sus sistemas de información.

1.3 Control de documentos

Los documentos requeridos por el Sistema de Seguridad de la Información (SSI) deben protegerse y controlarse. Para lograr este objetivo, las acciones necesarias a implementar son:

• Revisar y actualizar los documentos cuando sea necesario y aprobarlos nuevamente.

• Registrar todos los cambios o actualizaciones a los documentos en la tabla de control de cambios.

• Los registros de las actualizaciones o modificaciones en la tabla de control de cambio debe ser coincidente con el texto del respectivo documento.

• Los registros de las tablas de cambio deben ser legibles y fácilmente identificables en el documento respectivo.

• Se deberá controlar el uso no intencionado de documentos obsoletos.

• En caso de mantenerse los documentos por cualquier propósito, éstos deberán tener una adecuada identificación a efecto de diferenciarse de los vigentes.

Las versiones pertinentes de los documentos aplicables se encontrarán disponibles para quienes lo necesiten y serán almacenados y transferidos de acuerdo a los procedimientos aplicables a su clasificación.

2. CONTROL DE ACCESO

2.1 Reglas para el control de acceso

Las reglas para el control de acceso, estará documentado a través de los diferentes procedimientos de control de acceso a los recursos tecnológicos.

2.2 Gestión de identidades

Se deberá asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas de información. Se usará para la asignación de las credenciales de accesos a los diferentes sistemas, un formulario con el nombre del sistema, nombre usuario, contraseña temporal y la asignación de derechos al sistema y/o los servicios.

2.3 Responsabilidad de los usuarios

Todos los funcionarios o terceros que tengan un usuario en la plataforma tecnológica de la División Informática, deberán conocer y cumplir con su uso de esta Política específica, donde se dictan pautas sobre derechos y deberes con respecto al uso adecuado de los usuarios, así como políticas de protección de usuario desatendido, escritorio y pantalla limpia.

2.4 Control de Acceso a la Red

Las conexiones no seguras a los servicios de red pueden afectar a toda la institución, por lo tanto, se controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos.

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".

2.4.1 Política de utilización de los servicios de red

Se desarrollarán procedimientos para la activación y desactivación de derechos de acceso a las redes, los cuales comprenderán:

- Controlar el acceso a los servicios de red tanto internos como externos.
- Identificar las redes y servicios de red a los cuales se permite el acceso.
- Realizar normas y procedimientos de autorización de acceso entre redes.
- Establecer controles y procedimientos de administración para proteger el acceso y servicios de red.

2.4.2 Autenticación de usuarios para conexiones externas

La División Informática contempla como servicios de conexiones externas SSL, VPN y primarios para funcionarios que requieran conexión remota a la red de datos institucional.

2.4.3 Identificación de equipos en la Red

La División Informática controlará e identificará los equipos conectados a su red, mediante el uso de controladores de dominio, asignación manual de IP y portal cautivo para la conexión WIFI.

2.4.4 Protección de los puertos de configuración y diagnostico remoto

Los puertos que permitan realizar mantenimiento y soporte remoto a los equipos de red, servidores y equipos de usuario final, estará restringido a los administradores de red o servidores.

2.4.5 Separación de redes

La División Informática utilizará dispositivos de seguridad —firewalls“, para controlar el acceso de una red a otra.

La segmentación se realizará en equipos de enrutamiento mediante la configuración de lista de control de acceso y configuraciones de AP’s en los Routers.

2.4.6 Control de conexión de las redes

- La capacidad de descarga de cada usuario final será de 10 Mb.
- La seguridad para las conexiones WiFi será WPA2 o superior. Dentro de la red de datos institucional se restringirá el acceso a:
- Mensajería instantánea.
- La telefonía a través de internet.
- Correo electrónico comercial no autorizado.
- Descarga de archivos de sitio peer to peer.

- Conexiones a sitios de streaming no autorizado.

- Cualquier otro servicio que vulnere la seguridad de la red o degrade el desempeño de la misma.

2.4.7 Control de enrutamiento de red

El acceso a redes desde y hacia afuera de la División Informática cumplirá con los lineamientos del numeral 2.3 Control de acceso a la red y adicionalmente se utilizaran métodos de autenticación de protocolo de enrutamiento, rutas estáticas, traducción de direcciones y listas de control de acceso.

2.4.8 Control de enrutamiento de red

La División Informática, proveerá a través de sus ISPs (Proveedor de Servicio de Internet) el servicio de internet institucional, el cual será administrado por el proceso de direccionamiento tecnológico y será el único servicio de internet autorizado.

El uso de internet estará regulado por el Manual de buenas prácticas de Política de Seguridad de la Información.

2.5 Control de Acceso al Sistema Operativo

2.5.1 Registro de inicio seguro

El acceso a los sistemas operativos estará protegido, mediante un inicio seguro de sesión, que contemplará las siguientes condiciones:

- No mostrar información del sistema, hasta que el proceso de inicio se haya completado.
- No suministrar mensajes de ayuda, durante el proceso de autenticación.
- Validar los datos de acceso, una vez que se han diligenciado todos los datos de entrada.
- Limitar el número de intentos fallidos de conexión auditando los intentos no exitosos.
- No mostrar las contraseñas digitadas.
- No transmitir la contraseña en texto claro.

2.5.2 Gestión de contraseñas

La asignación de contraseñas se deberá controlar a través de un proceso formal de gestión a cargo del Área de soporte. Las recomendaciones son:

- No escribirlas en papeles de fácil acceso, ni en archivos sin cifrar.
- No habilitar la opción —recordar clave en este equipo“, que ofrecen los programas
- No enviarla por correo electrónico
- Nunca guarde sus contraseñas, en ningún tipo de papel, agenda, etc.
- Las contraseñas se deben mantener confidenciales en todo momento.
- No compartir las contraseñas, con otros usuarios.
- Cambia tu contraseña si piensas que alguien más la conoce y si ha tratado de dar mal uso de ella.
- Selecciona contraseñas que no sean fáciles de adivinar.
- Nunca grabes tu contraseña en una tecla de función o en un comando de caracteres pre-definido.
- Cambia tus contraseñas regularmente.
- No utilizar la opción de almacenar contraseñas en Internet.
- No utilizar contraseña con números telefónicos, nombre de familia etc.
- No utilizar contraseña con variables (soporte1, soporte2, soporte3 etc.)

2.5.3 Uso de utilitarios del sistema

El uso de utilitarios licenciados del sistema, estará restringido a usuarios administradores. Se establecerá una política a nivel del controlador de dominio, que no permita la instalación de software y cambios de configuración del sistema. Ningún usuario final, deberá tener privilegios de usuario administrador.

2.5.4 Uso de utilitarios del sistema

Después de cinco (5) minutos de inactividad del sistema, se considerará tiempo muerto y se bloqueará la sesión, sin cerrar las sesiones de aplicación o de red.

Los usuarios procederán a bloquear sus sesiones, cuando deban abandonar temporalmente su puesto de trabajo. Las estaciones de trabajo deberán quedar apagados al finalizar la jornada laboral o cuando una ausencia temporal supere dos (2) horas.

2.5.5 Limitación de tiempo de conexión

Por la misionalidad de la División Informática, no se limitará el tiempo de conexión, ni se establecerán restricciones en la jornada laboral.

2.5.6 Control de acceso a la información

El control de acceso a la información a través de una aplicación, se realizará a través de roles que administren los privilegios de los usuarios dentro del sistema de información.

El control de acceso a información física o digital, se realizará teniendo en cuenta los niveles de clasificación y el manejo de intercambio de información.

2.5.7 Control de acceso a la información

La División Informática, identificará según los niveles de clasificación de información cuales sistemas considera sensibles y que deberían gestionarse desde ambientes tecnológicos aislados e independientes.

Al aislar estos sistemas se debe prever el intercambio seguro de información, con otras fuentes de datos, ya que no se permite duplicar información en otros sistemas, siguiendo las directrices de fuentes únicas de datos.

2.6 Computación Móvil y Trabajo Remoto

Teniendo en cuenta las ventajas de la computación móvil y el trabajo remoto, así mismo el nivel de exposición a amenazas que pongan en riesgo la seguridad de la información institucional, a continuación se establecen directrices que permitirán regular el uso de la computación móvil y trabajo remoto:

2.6.1 Computación y comunicaciones móviles

Se entiende como dispositivos de cómputo y comunicación móviles, todos aquellos que permitan tener acceso y almacenar información institucional, desde lugares diferentes a las instalaciones.

El uso de equipos de cómputo y dispositivos de almacenamiento móviles, está restringido únicamente a los provistos por la institución.

CARLOS ANDRES ABRIL BRITO
Ingeniero de Sistemas

Biblioteca Virtual Calle 83 avenida Pedro Tafur Tel. (8) 2795992
E-mail: *imdrideportes@gmail.com* Pagina Wed: *www.imdri.gov.co*
Ibagué Tolima