ANEXO V

AUTENTICACIÓN, AUTORIZACIÓN Y CONTROL DE ACCESOS

1. OBJETIVO

Establecer las medidas técnicas y organizacionales aplicables sobre el acceso a los activos de información de la S.R.T..

Establecer las tareas y actividades que prevengan el acceso no autorizado a los activos de información, garantizando así la seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.

2. ALCANCE

Comprende todas las formas de acceso de aquellos a quienes se les haya otorgado permisos sobre los activos de información de la S.R.T., cualquiera sea la función que desempeñen, sea personal de la S.R.T. o terceros involucrados con el Organismo.

3. DEFINICIONES

***Acceso**:* Utilización de los recursos de un sistema de información.

Código fuente: es un conjunto de líneas de texto con los pasos que debe seguir la computadora para ejecutar un software. El mismo está escrito por un programador en algún lenguaje de programación, normalmente en forma de texto plano.

Contraseña: información confidencial y secreta que permite el acceso a algo, a alguien o a un grupo de personas. En general es un grupo de caracteres que permite la autenticación de un usuario, entidad o recurso.

Contraseña provisoria: Se asigna cuando los usuarios ingresan por primera vez a un sistema u olvidan su contraseña, y deben suministrarse solo una vez identificado el usuario inequívocamente.

Contraseñas críticas: Aquellas asignadas a personal técnico con cuentas con privilegios para llevar adelante tareas críticas como ser instalación de plataformas o sistemas, habilitación de servicios, actualización de software, configuración de componentes informáticos. Estas, debido a su naturaleza, se encontrarán protegidas por contraseñas con un mayor nivel de complejidad que el habitual.

Credencial de acceso o de inicio de sesión: son nombres de usuario y contraseñas gestionados que dan acceso a diversas aplicaciones.

Host: computadoras u otros dispositivos conectados a una red que proveen y utilizan servicios de ella.

Identificadores de usuario únicos: es un rango de valores que se asigna a un usuario para poder identificarlo de forma unívoca de manera que se lo pueda identificar por sus acciones evitando la existencia de múltiples perfiles de acceso para una misma persona.

Identificadores grupales o genéricos: cuando se asigna un rango de valores de forma genérica para que pueda ser utilizado por un grupo de usuarios.

Perfil de Usuario: contiene la información que el sistema necesita para permitir a un usuario iniciar una sesión en el sistema, para acceder a su propia sesión personalizada, y para acceder a funciones y objetos a los que se les haya otorgado autorización de acuerdo a su puesto de trabajo.

Privilegio: atributo, propiedad o capacidad asignada a una entidad o persona por una autoridad para el uso de un servicio controlado o restringido.

Sistemas multiusuario: son sistemas operativos que permiten que dos o más usuarios compartan los mismos recursos simultáneamente.

Usuario: un usuario informático es una persona que usualmente utiliza un servicio, pudiendo ser de red, aplicativo, de software, etc.

Utilitarios de sistemas: programas de los sistemas diseñados para realizar una función determinada, como, por ejemplo, un editor, un depurador de código o un programa para recuperar datos perdidos.

4. RESPONSABILIDADES

El Responsable de Seguridad de la Información (RSI) debe determinar con la Subgerencia de Sistemas (S.S.), según corresponda, las medidas de seguridad y los controles necesarios para la gestión de los accesos a todos los activos de información de la S.R.T..

Ambos deben definir y documentar lineamientos y procedimientos de seguridad a implementar respecto a la gestión de accesos y su monitoreo.

El RSI debe impulsar actividades de concientización a los usuarios en materia de seguridad sobre el uso apropiado de credenciales, contraseñas y equipamiento informático.

Por otro lado, debe controlar la asignación de accesos y privilegios a usuarios. Del mismo modo, debe verificar el cumplimiento de las pautas establecidas, relacionadas con control de accesos. Corresponde impulsar un proceso periódico de revisión de los derechos de acceso a la información y definir los eventos y actividades de usuarios al ser registrados.

La S.S. debe llevar adelante las medidas de seguridad definidas para la gestión de los accesos a todos los activos de información de la S.R.T..

Le corresponde también evaluar los riesgos existentes en las instalaciones de procesamiento de información, de acuerdo a los criterios establecidos por el RSI y con el objeto de definir medios de monitoreo y tecnologías de identificación y autenticación de usuarios.

Asimismo, debe coordinar con la Subgerencia de Recursos Humanos (S.R.H.) y con los Titulares de las Unidades Organizativas la gestión de altas, modificaciones y bajas de cuentas del personal S.R.T. y sus privilegios asociados.

Por otro lado, debe implementar procedimientos para la activación y desactivación de derechos de acceso a las redes y métodos de autenticación y control de acceso definidos en los sistemas, bases de datos y servicios.

Asimismo, debe llevar a cabo los registros de eventos y actividades que sean definidos oportunamente.

La S.R.H. debe comunicar a la S.S. todas las novedades respecto de las altas, modificaciones y bajas del personal de la S.R.T. que pudieran tener impacto directo en los accesos a los sistemas de la S.R.T..

Los Titulares de las Unidades Organizativas deben evaluar los riesgos a los cuales se expone la información de la cual son propietarios, de acuerdo a los criterios establecidos por el RSI, con el objeto de ponderar el acceso del personal a su cargo a los activos de información de la S.R.T..

Deben analizar y aprobar el acceso del personal a su cargo a los servicios, recursos de red y a conectividad. Asimismo, deben aprobar y solicitar la asignación de privilegios al personal, en caso

de ser necesario, y colaborar en el proceso formal y periódico de revisión de los derechos de acceso a la información.

Por último, deberán velar por el uso responsable de la información que se gestiona en sus áreas de dependencia, sea por personal a su cargo o por terceros asociados a sus procesos.

5. CONTENIDO

5.1 GESTIÓN Y ADMINISTRACIÓN DE ACCESOS

5.1.1 Administración de privilegios de acceso

Los sistemas que requieren protección contra accesos no autorizados, deberán prever una asignación de privilegios controlada mediante un proceso de autorización formal. Para ello se deberá limitar y controlar la asignación y el uso de privilegios de acceso, estableciendo criterios que contemplen mínimamente los siguientes aspectos:

1. La identificación de privilegios asociados a cada sistema (sistema operativo, sistema de administración de bases de datos y aplicaciones), y los roles/ perfiles del personal a los cuales deben asignarse los permisos;
2. La asignación de privilegios a usuarios utilizando el principio de “necesidad de saber”, es decir, en la medida en que sean requeridos para las actividades y tareas que cada persona debe llevar adelante;
3. Un proceso de autorización y de registro de todos los privilegios asignados;
4. Promover el desarrollo y uso de Reglas / Directivas disponibles en los sistemas para evitar la necesidad de otorgar privilegios a los usuarios de manera manual;
5. La administración de las contraseñas y permisos de acceso a los sistemas.

5.1.2 Asignación de cuentas y contraseñas de usuarios

Se deberá hacer una adecuada y oportuna gestión de las altas, modificaciones y bajas de cuentas de usuario y privilegios. Para ello se elaborará un procedimiento de registro de usuarios para otorgar, modificar y revocar el acceso a todos los sistemas, bases de datos y servicios de información multiusuario, el cual debe contener, entre otros aspectos:

- El otorgamiento de identificadores de usuario únicos;
- Un análisis de las solicitudes de identificadores grupales, solo permitiéndolas cuando sean convenientes para el trabajo a desarrollar con motivos operativos y bajo la expresa aprobación de los titulares de las unidades organizativas donde se desempeñen aquellas tareas;
- El otorgamiento de un adecuado nivel de acceso de acuerdo con el propósito de la función del usuario;
- La autorización formal para el uso del sistema, base de datos o servicio de información;
- Un compromiso por parte de los usuarios, señalando que comprenden y aceptan las condiciones para el acceso, incluyendo el mantener sus contraseñas personales en secreto y las contraseñas de los grupos de trabajo, en caso de existir, exclusivamente entre los miembros del grupo;
- La necesidad de que todas las áreas intervinientes en el proceso estén informadas de las novedades que pudieran impactar en las cuentas de los usuarios, incluyendo los cambios de revista, funciones y cese de actividad;
- Las justificaciones y aprobaciones para aquellos casos que se consideren como excepciones;

- Un proceso ágil para modificar o dar de baja los permisos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización, se desvincularon del S.R.T. o sufrieron la pérdida/robo de sus credenciales de acceso.

Por su parte, la asignación de cuentas y contraseñas se debe establecer a través de un proceso de administración formal. Para esto, se deberán establecer mecanismos que contemplen los siguientes aspectos:

1. Generar contraseñas provisorias seguras y garantizar la seguridad en su entrega;
2. Garantizar que las contraseñas provisorias que se les asigna a los usuarios, la primera vez que ingresan al sistema, o en caso de olvido de éstas, sean modificadas una vez utilizadas;
3. Almacenar las contraseñas sólo en sistemas informáticos protegidos;
4. Establecer reglas para el mantenimiento del directorio de usuarios de la S.R.T.;
5. Llevar adelante un monitoreo periódico sobre el directorio de usuarios con el objeto de identificar inconsistencias, como por ejemplo cuentas redundantes y/o inactivas.

5.1.3 Cuentas con privilegios especiales

En los diferentes ambientes de procesamiento de información existen cuentas de usuarios con privilegios, con las cuales es posible efectuar actividades críticas sobre los sistemas y la infraestructura de procesamiento. Dichas cuentas no serán de uso habitual (diario), sino que sólo serán utilizadas ante una necesidad específica de realizar alguna tarea que lo requiera.

Se deberán definir los procedimientos para la administración de dichas contraseñas críticas que contemplen:

- Las causas que justifiquen su uso, así como el nivel de autorización requerido;
- El nivel de seguridad y la modalidad de otorgamiento;
- La modalidad de resguardo;
- El registro y monitoreo de este tipo de credenciales, y la asignación de un responsable de las actividades que se efectúen con la misma;
- La modalidad de renovación y la fijación de un período de uso;
- El registro de las actividades que se efectúen con las cuentas críticas.

5.1.4 Revisión de Derechos de Acceso de Usuarios

A fin de mantener un control eficaz del acceso a los sistemas e infraestructura de procesamiento, se deberá establecer un proceso formal de monitoreo de los derechos de acceso a los usuarios. En esa línea, se deberán establecer lineamientos que contemplen los siguientes controles:

- Revisión de permisos de acceso de los usuarios, determinando intervalos de revisión regulares;
- Revisión de autorizaciones de cuentas con privilegios especiales, determinando intervalos de revisión regulares;
- Revisión de asignaciones de privilegios, determinando intervalos de revisión regulares.

5.2 USO RESPONSABLE DE DATOS DE AUTENTICACIÓN Y DE DISPOSITIVOS INFORMÁTICOS

5.2.1 Gestión de credenciales de acceso

Se deberá informar, concientizar y requerir de los usuarios que posean credenciales de acceso y/o dispositivos brindados por la S.R.T., un uso responsable de los mismos, con el fin de prevenir

potenciales accesos no autorizados. Asimismo, se deberán elaborar lineamientos que, mínimamente, incluyan las siguientes consideraciones:

- El mantener las contraseñas en secreto, de forma segura y no compartirlas;
- La solicitud de cambio de contraseñas, siempre que exista un posible indicio de compromiso, tanto de los sistemas como de las mismas;
- El cambio de contraseñas cuando le sea requerido a los usuarios por los propios sistemas;
- La notificación mediante los canales establecidos de incidentes relacionados con el compromiso de contraseñas y/o dispositivos electrónicos por pérdida o robo;
- La aplicación de buenas prácticas sobre uso aceptable de dispositivos electrónicos y de pantallas y escritorios limpios, incluyendo evitar dejar los equipos desatendidos y la conclusión de sesiones activas al finalizar sus tareas.

5.2.2 Desconexión de equipamiento informático por inactividad

Las computadoras o equipamiento informático se deberán apagar después de un periodo definido de inactividad o “tiempo muerto”, para evitar así el acceso de personas no autorizadas. Se deberán establecer mecanismos específicos para el bloqueo automático de las computadoras personales (PC), sin posibilidad de apertura más que por el usuario identificado.

5.3 CONTROL DE ACCESO A LA RED

5.3.1 Criterios de utilización de los servicios de Red

Se desarrollarán procedimientos específicos para la activación y desactivación de derechos de acceso a las redes.

Se controlará el acceso a los servicios de red tanto internos como externos, garantizando que aquellos que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos.

5.3.2 Autenticación de Usuarios para conexiones externas

Se deberá incorporar controles para aquellos usuarios que se conecten de manera remota. Para esto, se deberá considerar:

- La implementación de mecanismos que permitan una conexión segura;
- Estrategias para el acceso a la información;
- Las aprobaciones necesarias para establecer la conexión remota.

5.3.3 Acceso a Internet

El acceso a Internet será utilizado solo con propósitos autorizados o con el destino por el cual fue provisto. Se establecerán procedimientos para solicitar y aprobar accesos a Internet, así como para los permisos de navegación. Asimismo, se deberán definir pautas de utilización de Internet para todos los usuarios.

5.4 CONTROL DE ACCESO AL SISTEMA OPERATIVO

5.4.1 Procedimientos de conexión de PCs y Servidores

Se deberá establecer un procedimiento de conexión e identificación a las computadoras y servidores que contemple mecanismos para asegurar el acceso solo de usuarios autorizados, considerando las siguientes directrices:

- Divulgar la mínima información posible acerca del sistema, a fin de evitar que provea de asistencia innecesaria a usuarios no autorizados;
- Mantener en secreto los nombres de *host* de sistemas o aplicaciones hasta tanto se lleve a cabo con éxito el proceso de conexión;
- Evitar brindar mensajes de ayuda que pudieran asistir a un usuario no autorizado durante el procedimiento de conexión, validando la información de la conexión sólo al completarse la totalidad de los datos de entrada. Si surge una condición de error, el sistema no debe indicar qué parte de los datos es correcta o incorrecta;
- Limitar el número de intentos de conexión no exitosos permitidos y, cuando sea posible, registrarlos. Se impedirán otros intentos de identificación, una vez superado el límite permitido;
- Establecer el tiempo máximo permitido para el procedimiento de conexión. Si este es excedido, el sistema deberá finalizar la conexión.

5.4.2 Sistema de administración de contraseñas

Se deberá contar con sistemas de administración de contraseñas que contemplen:

- Imponer el uso de contraseñas individuales;
- Permitir que los usuarios seleccionen y cambien sus propias contraseñas (luego de cumplido el plazo mínimo de mantenimiento de las mismas);
- Imponer una selección de contraseñas robustas;
- Imponer cambios periódicos en las contraseñas;
- Modificar todas las contraseñas predeterminadas.

5.4.3 Uso de utilitarios de sistema operativo

Existen sistemas que disponen de uno o más programas utilitarios que podrían tener la capacidad de pasar por alto los controles de sistemas y aplicaciones. Es por ello que, ante la necesidad de su uso, el mismo deberá ser debidamente justificado, limitado y controlado.

5.5 CONTROL DE ACCESO A LAS APLICACIONES Y CÓDIGO FUENTE

5.5.1 Restricción del acceso a los aplicativos

Se deberá definir e implementar un procedimiento para la gestión de todos los usuarios en sistemas aplicativos. Asimismo, se deberán aplicar los siguientes controles, para brindar apoyo a los requerimientos de limitación de accesos:

1. Proveer una interfaz para controlar el acceso a las funciones de los sistemas de aplicación;
2. Restringir el conocimiento de los usuarios acerca de la información o de las funciones de los sistemas de aplicación a las cuales no sean autorizados a acceder;
3. Controlar los derechos de lectura, escritura, supresión y ejecución en el acceso de los usuarios;
4. Restringir el acceso a la información sin la utilización del sistema encargado de su procesamiento, es decir, la modificación directa del dato almacenado.

5.5.2 Acceso al código fuente

Se deberá restringir y controlar el acceso al código fuente de las aplicaciones de software desarrolladas en la S.R.T. solo al personal informático autorizado, con el fin de evitar que sean introducidos cambios sin la debida autorización y control de las áreas involucradas, como así también copias y descargas no autorizada del código fuente. Para esto, se deberá definir y tener en

cuenta los perfiles de usuario que requieren acceso al mismo y el ambiente de trabajo donde se requiere dicho acceso.

5.6 REGISTRO Y MONITOREO

5.6.1 Registro de eventos

Se deberá establecer una estrategia para la generación de los registros de eventos relacionados a los accesos, que contengan excepciones y otros eventos relativos a la seguridad. Asimismo, se deberá definir la información mínima requerida en cada registro con el fin de poder llevar a cabo un monitoreo.

5.6.2 Monitoreo del uso de los sistemas

Se definirán procesos con el fin de monitorear el uso de los sistemas donde se encuentre el procesamiento de la información. Dichos procesos deberán establecer el alcance y qué registros tendrá en cuenta para su monitoreo, considerando los factores de riesgo asociados, como ser la criticidad de los procesos que se encuentran en las aplicaciones.

5.6.3 Sincronización de relojes

Se deberá disponer de un procedimiento de ajuste de relojes, el cual indicará también su verificación contra una fuente externa del dato y la modalidad de corrección, a fin de garantizar la exactitud de los registros.

República Argentina - Poder Ejecutivo Nacional
1983/2023 - 40 AÑOS DE DEMOCRACIA

Hoja Adicional de Firmas
Anexo firma conjunta

Número: IF-2023-66577970-APN-GT#SRT

CIUDAD DE BUENOS AIRES
Viernes 9 de Junio de 2023

Referencia: ANEXO V Autenticación, Autorización y Control de Accesos-EX-2023-56789749- -APN-GT#SRT

El documento fue importado por el sistema GEDO con un total de 8 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2023.06.09 12:39:34 -03:00

Diego Maximiliano Segovia
Subgerente
Subgerencia de Sistemas
Superintendencia de Riesgos del Trabajo

Digitally signed by Gestion Documental Electronica
Date: 2023.06.09 12:45:19 -03:00

Marcelo Angel Cainzos
Gerente
Gerencia Técnica
Superintendencia de Riesgos del Trabajo

Digitally signed by Gestion Documental Electronica
Date: 2023.06.09 12:45:21 -03:00