Políticas de Acceso a Infraestructura

1. Introducción

Los recursos de infraestructura de TI conforman la base para brindar soporte al procesamiento y almacenamiento de la información del Gobierno de San Juan. La correcta administración de los accesos de los usuarios a estos recursos es fundamental para garantizar la seguridad de la información. En adelante, al mencionar la seguridad de la información, este documento se refiere a su debida confidencialidad, integridad y disponibilidad. Para asegurar estos tres ítems componentes de la seguridad de la información es necesario identificar a cada una de las personas que utilizan los recursos de infraestructura de TI, además de determinar los permisos de acceso que tienen, tuvieron o podrían tener, dependiendo de las funciones que ellas desempeñan en el Gobierno de San Juan.

En este documento se establecen los lineamientos principales a tener en cuenta al momento de otorgar, modificar o remover accesos de usuarios a dichos recursos.

2. Objetivo

Establecer los lineamientos que permitan asegurar una adecuada administración de los accesos de usuarios a los recursos de infraestructura de TI del Gobierno de San Juan.

3. Alcance

Todos de usuarios que requieran acceso a los recursos de infraestructura de TI del Gobierno de San Juan, incluyendo accesos a:

- Base de datos
- Sistemas que administren algún tipo de información crítica.
- Dispositivos de redes
- Infraestructura Convergente
- Dispositivos de seguridad (p.ej. Firewall, SIEM, etc.)

a) Origen físico/lógico para los Accesos Privilegiados

Cualquier tipo de gestión de los recursos de Infraestructura TI deberá ser realizada sólo desde intranet (red 10.0.0.0/8), en aquellos casos que el recurso permita una gestión por https se podrá gestionar excepcionalmente mediante VPN de manera directa.

Bajo ninguna circunstancia deberá estar permitida la gestión desde Internet, como así también no deberá existir ningún tipo de acceso directo al recurso TI por puertos/protocolos de gestión (excepto https) mediante VPN o cualquier tipo de herramienta de administración remota.

Para el caso que sea necesaria una gestión de a fuera de la Intranet (red 10.0.0.0/8) se le habilitará una VPN al Administrador a una PC (física o virtual) en la Intranet y de ahí podrá gestionar el recurso TI.

Cualquier PC (física o virtual) con permiso para gestionar un recurso TI deberá estar unida al dominio y con la herramienta instalada de protección de punto final provista por la Dirección de Ciberseguridad.

Cualquier Servidor sea físico o virtual que contenga servicios del Gobierno de San Juan, así sea para uso del agente público o un servicio hacia el ciudadano, deberán estar alojados en un Data Center que cumpla con las políticas de accesos mencionadas en este documento.

b) Cuentas de Accesos Privilegiados

Las cuentas mencionadas en este alcance son consideradas cuentas de **accesos privilegiados** puesto que tienen la capacidad de realizar alguna o varias de las siguientes tareas:

- Crear cuentas / ID de usuario y/o grupos
- Otorgar o cambiar el acceso a cuentas / ID de usuario (incluyendo revocar / deshabilitar)
- Restablecer contraseñas
- Acceder directamente bases de datos o sistemas de información
- Cambiar la configuración técnica o parámetros funcionales de la aplicación y que puede afectar la funcionalidad del componente de la aplicación y / o la infraestructura, así como las características técnicas (por ejemplo, seguridad y rendimiento)

c) Cuentas incluidas dentro del alcance de este documento:

Este listado no es taxativo, puede ser ampliado o mejor especificado en cada nueva versión de este documento.

- Cuentas de usuario nombradas
- Cuentas predeterminadas del sistema (sembradas)
- Cuentas de servicio
- Cuentas de administrador de sistema TIC
- Cuentas de administrador de base de datos
- Cuentas de administrador de dominio
- Cuentas de administrador local
- Cuentas de administrador de aplicación
- Cuentas de administrador de estaciones de trabajo

d) De acuerdo al estándar establecido en este documento:

- Deben ser cuentas de usuario únicas e individuales.
- No deben usarse con fines no administrativos y deben asignarse a los delegados apropiados.
- Generalmente están restringidas para ser asignadas al personal de soporte del Equipo de Infraestructura Tecnológica, o personas aprobadas que no tienen responsabilidades financieras clave en un entorno de producción.
- Todas las solicitudes de acceso privilegiado deben ser aprobadas por el Propietario de la Aplicación (por lo general, un miembro del Equipo de Infraestructura Tecnológica).

4. Contenido

a) Condiciones requeridas para el acceso a recursos de TI

Todo el software que sirva administrar los ítems listado en el punto 3 (en adelante, recurso de infraestructura TI) y que se encuentre en producción deberá contar con los permisos de acceso privilegiado correspondientes. Esto permitirá controlar el acceso a funcionalidades e información a través de una adecuada segregación de dichos accesos conforme a los niveles de criticidad que el mencionado software posea.

b) Administración de accesos de usuarios a recursos de TI

Lineamientos que se deberán cumplir para el acceso de usuarios a los recursos de infraestructura de TI del Gobierno de San Juan:

- Siempre que resulte posible se utilizará una política Single SignOn (SSO), mediante el Servicio de Dominio. En el ítem a continuación se detalla la política de contraseña estándar que se debe usar para todas las autenticaciones, independientemente de la aplicación de SSO.

c) Política de Contraseña Estándar

Todas las contraseñas utilizadas dentro del ámbito de acceso a servicios, aplicaciones e infraestructura del Gobierno de San Juan deberán seguir el siguiente estándar. Las eventuales excepciones a este estándar deben ser documentadas y aprobadas por la Dirección de Ciberseguridad:

- Historial de contraseñas deshabilitado
- Edad máxima de la contraseña: 180 días
- Edad mínima de la contraseña: 1 día
- Longitud mínima de la contraseña: 8 caracteres
- La contraseña debe cumplir con los requisitos de complejidad: habilitada
- Umbral de bloqueo de cuenta: 10 intentos fallidos
- Duración del bloqueo de la cuenta: indefinido

Nota importante:

* Las aplicaciones, sistemas o servicios de aplicación deberán utilizar cuentas de servicio siempre que necesiten interactuar con otros recursos de información, aplicaciones, sistemas o servicios. Las cuentas de acceso privilegiado no deben de ninguna forma ser utilizadas con esta finalidad.

d) Solicitud de Alta, Baja o Modificación

La solicitud de alta, baja o modificación de accesos deberá cumplir con los siguientes requisitos:

- Será realizada por el Director (o su equivalente o superior jerárquico) de la repartición a la que pertenece el usuario requirente, a través de una nota dirigida al Director General responsable del recurso de infraestructura TI, con el formulario correspondiente. El mismo y en conjunto con el Director de la Dirección de Ciberseguridad, aprobarán la solicitud.
- La solicitud no puede ser aprobada por la misma persona que la inicia, a menos que haga esta gestión en nombre de otra persona y se cumplan todos los pasos de autorización jerárquica para aprobar el acceso solicitado.
- La asignación documentada de delegados (Delegación de Autoridad de Aprobación) se reconoce como un método apropiado de autorización, sin embargo, la responsabilidad de esta asignación y de la tarea delegada permanecen con el individuo original.

i. Solicitud de alta, baja o modificación de acceso.

La solicitud de alta, baja o modificación de acceso deberá contener como mínimo la siguiente información:

- Único ID.
- Nombre, apellido.
- Repartición de pertenencia.

- Recurso de infraestructura de TI al que se solicita acceder o modificar el acceso.
- Perfil requerido de acceso o modificación.
- Justificación de la solicitud.
- Condiciones de uso del acceso.

ii. Consideraciones a tener en cuenta

Las siguientes consideraciones serán contempladas en el proceso de alta, baja o modificación:

- Los ID de usuario no deben ser reutilizados en ningún momento y bajo ninguna causa o motivo.
- Todo el personal temporal que requiera acceso a recursos de información del Gobierno de San Juan (incluyendo, pero no limitado a un acceso estándar, elevado o privilegiado) debe seguir este estándar. Su solicitud debe contar con una fecha de inicio y finalización claramente especificadas para que la cuenta se deshabilite en la fecha determinada por el solicitante y el gerente aprobador, supervisor, equivalente o delegado.
- Cualquier cambio, modificación o alteración en el acceso debe ser comunicado de manera fehaciente a la Dirección de Ciberseguridad.
- La cuenta de usuario del personal transferido a diferentes departamentos o ubicaciones gubernamentales debe documentarse debidamente y aprobarse por las autoridades competentes de dichas reparticiones, en forma previa a la obtención de los privilegios adecuados. Es la responsabilidad del nuevo gerente, supervisor, equivalente o delegado identificar y definir los privilegios de acceso solicitados para el usuario (incluidos los temporales o de desactivación de acceso) y que son expresamente necesarios para la realización de su tarea asignada administrativamente mediante resolución del área correspondiente.

Nota importante:

* Los formularios de solicitud de alta, baja o modificación deberán contener espacio para llenado obligatorio en campos de tiempo predefinido de caducidad del acceso, anulación de acceso en caso de cambio de repartición de pertenencia del usuario, y otros, y espacio opcional para cuando existan observaciones sobre el uso del acceso solicitado.

iii. Solicitud de baja de acceso

La solicitud de baja de acceso deberá contener como mínimo la siguiente información:

- Único ID.
- Nombre, apellido.
- Repartición de pertenencia.
- Recurso de infraestructura de TI al que se solicita remover el acceso.
- Perfil a dar de baja.
- Justificación de la solicitud.
- Condiciones de baja del acceso.

Nota importante:

* Las bajas de accesos se podrán realizar de manera manual o automatizada al momento de caducidad de vigencia de pedido de acceso, desactivación de usuarios o cualquier otra situación que sea causa del cese de funciones. El solicitante debe indicar si la baja de acceso es temporal o permanente.

iv. Bajas por desvinculación

Si la baja del usuario se debe a su desvinculación del Gobierno de San Juan, el Organismo al cual pertenece deberá notificar inmediatamente y de forma fehaciente a la Dirección de Ciberseguridad para que ésta verifique todos los accesos que el usuario tiene asignado y realice la remoción de los mismos.

e) Autorización

Las solicitudes de altas, bajas y modificaciones de accesos a recursos de infraestructura de TI requieren la autorización del Director del área responsable del recurso de infraestructura TI y del Director de Ciberseguridad, pudiendo el Director de Ciberseguridad delegar esta atribución de manera formal en personal de su repartición.

Sólo se podrá aprobar o rechazar la información recibida, no pudiendo modificar la misma una vez recibida.

En el caso de que el pedido de acceso no satisfaga alguna de las condiciones del formulario de solicitud (justificación de uso, repartición de pertenecía del usuario u otro), o no sea determinado como excepción autorizada por el Director de Ciberseguridad, el mismo será rechazado y devuelto, indicando el motivo de rechazo.

En todos los casos, luego de implementar los accesos autorizados, se dará aviso formal a los solicitantes.

La Dirección encargada del recurso de infraestructura TI debe mantener un registro de los usuarios de su repartición, sus permisos o perfiles otorgados, las solicitudes de acceso y autorizaciones correspondientes. Esta documentación podrá ser solicitada en cualquier momento y bajo cualquier condición por la Dirección de Ciberseguridad.

f) Administración de contraseñas

- El usuario no debe compartir ni publicar ninguna de sus contraseñas de ninguna manera.
- Las contraseñas temporales deben transmitirse de manera segura utilizando para tal fin los medios que se detallan a continuación:
    - Generar un vínculo conteniendo la información crítica mediante la herramienta https://qlink.it/

  - Enviar el vínculo generado mediante un correo electrónico con remitente y destinatario pertenecientes al dominio del gobierno de San Juan (@sanjuan.gov.ar)
  - Excepcionalmente y sólo en el caso de que el vínculo contenga información de un nuevo usuario de correo electrónico del dominio San Juan (@sanjuan.gov.ar), el destinatario podrá ser un correo personal (Gmail, Hotmail, etc.).
- Todos los usuarios deben cambiar su contraseña temporal el primer inicio de sesión.
- Se prohíbe la autenticación automática mediante scripts o macros que inserten en los formularios de acceso su ID de usuario y su contraseña.
- La visualización e impresión de contraseñas debe enmascararse, suprimirse u ocultarse de modo que asegure su integridad ante la presencia de terceros.
- Todas las contraseñas predeterminadas suministradas por el proveedor deben cambiarse antes de que se utilice cualquier recurso vinculado a este proveedor.
- Cuando no se pueden cambiar las contraseñas predeterminadas, un control compensatorio deben definirse, establecerse, revisarse, documentarse y aprobarse.

g) Responsable del Alta/Baja/Modificación

Una vez autorizado el encargado de realizar la tarea será el Superior Jerárquico, o algún miembro de su equipo con **accesos privilegiados,** del área responsable del recurso de infraestructura TI.

h) Revisión periódica de usuarios activos

La Dirección de Ciberseguridad podrá sin aviso realizar una revisión de los accesos otorgados a los usuarios en los recursos de infraestructura de TI, a fin de identificar que los mismos sigan activos, solicitando a la Dirección responsable del recurso TI los registros correspondientes.

i) Usuarios Generales

En primera instancia por temas de seguridad y de performance solo tendrán acceso a la infraestructura aquellos usuarios pertenecientes al área responsable de la operación y mantenimiento del recurso TI (ver listado en la tabla a continuación). Sólo en caso excepcional y justificado y mediante una autorización fehaciente se podrá autorizar a personal de otra área para el acceso mencionado.

Recurso TI	Área	Dirección
Sistemas	DPI	DPI
Base de datos	Operaciones	DCS
Redes de Datos	Redes de Datos	DRyCT
Infraestructura Convergente	Operaciones	DCS
Dispositivos de Seguridad	Ciberseguridad	DCS

Anexo 1

Cambios en base de datos por fuera de una aplicación

Toda modificación de los datos operativos del ambiente de producción por fuera del software de aplicación y que se realice por excepción justificada y aprobada, deberá reflejar el cambio en los registros de eventos correspondientes (hoja de cambio), como requisito obligatorio para la ejecución de dicha modificación.