Política Específica de Gestión de Accesos

ÍNDICE

1. OBJETIVO, ALCANCE Y USUARIOS

El objetivo del presente documento es definir reglas de acceso para diversos sistemas, equipos, instalaciones e información en base a los requerimientos de negocios y de seguridad.

Este documento se aplica a todo el alcance del Sistema de Gestión de Seguridad de la Información (SGSI); es decir, a todos los sistemas, equipos, instalaciones e información utilizados dentro del alcance del SGSI.

Los usuarios de este documento son todos los colaboradores de DACTA.

2. DOCUMENTOS DE REFERENCIA

- NTP-ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información, clausulas 5.15, 5.16, 5.17, 5.18, 5.33, 7.2, 7.4, 8.2, 8.3, 8.4, 8.5, 8.11, 8.23.

3. POLÍTICA ESPECÍFICA

Esta Política determina gestionar los accesos a la información. Se debería controlar el acceso a la información y los procesos del negocio sobre la base de los requisitos de seguridad.

El principio básico es que el acceso a todos los sistemas, redes, servicios e información está prohibido salvo que sea expresamente permitido a usuarios individuales o a grupos de usuarios. Debe existir un procedimiento de registro de usuarios para cada sistema y servicio.

Todo trabajador de DACTA o tercero para el desempeño de sus funciones, se compromete a lo siguiente:

- Es responsabilidad del Coordinador TI implementar y gestionar los controles para el acceso físico y lógico a la red, a los equipos de comunicaciones, los dispositivos de almacenamiento y a los equipos de cómputo.
- El Oficial de seguridad, en coordinación con el Gerente de línea serán los encargados de verificar el cumplimiento de las políticas de seguridad al momento de implementar los controles de acceso.
- La implementación de redes inalámbricas está restringida. No obstante, de requerirse, el Coordinador TI debe asegurarse que las redes inalámbricas cuenten con un servicio independiente de Internet.
- Las redes inalámbricas no podrán compartir la misma red donde se encuentran los servidores ni de las computadoras del personal de DACTA.
- El Oficial de Seguridad debe verificar periódicamente los controles de acceso para los usuarios provistos por terceras partes, con el fin de revisar que dichos usuarios tengan acceso permitido únicamente a aquellos recursos de red y servicios de la plataforma tecnológica para los que fueron autorizados.
- Los colaboradores, antes de contar con acceso lógico por primera vez a la red de datos de DACTA, deben contar con el formato de solicitud de creación de cuentas de usuario debidamente autorizado.
- El coordinador TI, establecerá y controlará los privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información de la organización. Así mismo, velará porque los colaboradores y el personal provisto por terceras partes tengan acceso

únicamente a la información necesaria para el desarrollo de sus labores y la asignación de los derechos de acceso esté regulada por procedimientos establecidos para tal fin.

- Los usuarios de los recursos tecnológicos y los sistemas de información de DACTA, realizarán un uso adecuado y responsable de dichos recursos y sistemas, salvaguardando la información a la cual les es permitido el acceso.
- El Coordinador TI, velará porque los recursos de la plataforma tecnológica y los servicios de red de la organización sean operados y administrados en condiciones controladas y de seguridad, que permitan un monitoreo posterior de la actividad de los usuarios administradores, poseedores de los más altos privilegios sobre dichos plataforma y servicios.
- Las jefaturas de DACTA como propietarias de los sistemas de información y aplicativos que apoyan los procesos y áreas que lideran, velarán por la asignación, modificación y revocación de privilegios de accesos a sus sistemas o aplicativos de manera controlada.
- El Coordinador TI como responsable de la administración de los sistemas de información y aplicativos, propenderá para que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico. Asimismo, coordinará con el responsable de Desarrollo porque los desarrolladores, tanto internos como externos, acojan buenas prácticas de desarrollo seguro en los productos generados.
- Debe realizarse el registro de recursos informáticos externos. Al ingresar a las instalaciones de DACTA todo recurso informático debe registrarse.

3.1. LINEAMIENTOS PARA EL PERFIL DE LOS USUARIOS

- Los usuarios y contraseñas asignados a los trabajadores de DACTA son personales e intransferibles.
- Para la Gestión interna de DACTA no se permite utilizar usuarios genéricos, salvo excepciones debidamente analizadas y autorizadas por el Oficial de Seguridad de la Información.
- Toda cuenta de usuario debe tener asignada una contraseña.
- El colaborador de DACTA es responsable de la actividad asociada a su usuario. DACTA, en lo posible, debe registrar la actividad de los usuarios, para su posterior control en caso de ocurrencia de incidentes.
- Las contraseñas deben requerir cierto nivel de complejidad mínimo y no pueden estar asociadas a datos personales que permitan su deducción, como, por ejemplo: nombres propios, nombre de usuario, números de documento, dirección, teléfono, etc.
- Las contraseñas mínimamente deben cumplir con los siguientes requerimientos:
  - Longitud mínima de 7 caracteres.
  - Estar formada por las características siguientes:
    - Caracteres alfabéticos en mayúsculas y/o minúsculas.
    - Caracteres numéricos.
    - Caracteres especiales o extendidos.
- Las contraseñas deben tener un tiempo limitado de vigencia o validez. La validez de las contraseñas no podrá superar los 12 meses. Dependiendo de la criticidad del sistema de información al cual se accede, se deberá manejar periodos más acotados.
- Se debe forzar al usuario a cambiar su contraseña en su primer uso y/o luego de ser asignada por el administrador del sistema.
- Se debe realizar el bloqueo de la cuenta luego de reiterados intentos fallidos de inicio de sesión.

- Se debe garantizar que cuando un usuario con accesos privilegiados deja la posición a otra persona, el nuevo usuario se vea obligado a cambiar las contraseñas a los respectivos activos a donde tenga acceso.

3.2. LINEAMIENTOS PARA LOS USUARIOS DE PERFIL CON PRIVILEGIOS ESPECIALES

- La asignación de una cuenta de usuario privilegiado, tipo Administrador, Admin o root, debe ser autorizada formalmente por el Gerente del área respectiva y refrendada por el Oficial de Seguridad de la Información. La solicitud debe ser acompañada de la justificación debidamente sustentada y se debe especificar la vigencia de estos derechos. Debe cumplir con los pasos para altas, bajas y modificaciones de usuarios con acceso privilegiado.
- Las cuentas de usuario privilegiado sólo deben ser otorgadas al personal que en el cumplimiento de sus funciones amerita contar con privilegios especiales de acceso.
- Los accesos realizados con cuentas de usuario privilegiados deben ser registrados y auditados permanentemente. Una cuenta de usuario privilegiado sólo podrá ser utilizada en la actividad de administración o configuración del sistema para la cual se requieren dichos privilegios.
- Las cuentas Administrador, admin o root, no podrán ser utilizadas en actividades rutinarias para la que exista un perfil de menores privilegios que lo permita.
- El acceso privilegiado debe realizarse desde dispositivos debidamente fortalecidos para tal fin.
- DACTA debe contar con pasos definidos que cubran los siguientes puntos:
  - Altas, bajas y modificaciones de usuarios y derechos de acceso lógico.
  - Altas, bajas y modificaciones de usuarios con acceso privilegiado (gestión y autorización).
  - Autorizaciones de acceso lógico.
  - Revisión de los derechos de acceso lógico

3.3. GESTIÓN DE PRIVILEGIOS

Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente. Los sistemas multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal. Se deben tener en cuenta los siguientes pasos:

- Identificar los privilegios asociados a cada producto del sistema, por ejemplo, sistema operativo, sistema de administración de bases de datos y aplicaciones y las categorías de personal a las cuales deben asignarse los productos software.
- Asignar los privilegios a individuos sobre la base de la necesidad de uso y evento por evento, por ejemplo, el requerimiento mínimo para su rol funcional.
- Mantener un proceso de autorización y un registro de todos los privilegios asignados.
- Los privilegios no deben ser otorgados mientras no se haya culminado el proceso formal de autorización.
- Promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.

Los propietarios de información serán los encargados de aprobar la asignación de privilegios a sus usuarios, lo cual será supervisado por el Oficial de Seguridad de la

Información.

3.4. REVISIONES PERIÓDICAS DE LOS DERECHOS DE ACCESO

A fin de mantener un control eficaz del acceso a los datos y servicios de información, todo propietario de la información deberá llevar a cabo un proceso formal de revisión, a intervalos regulares (mayor a 6 meses), a fin de validar los derechos de acceso de sus usuarios. Se deberán contemplar los siguientes controles:

- Revisar los derechos de acceso de los usuarios a intervalos regulares (mayor a 6 meses).
- Revisar las autorizaciones de privilegios especiales de derechos de acceso a intervalos regulares (recomendable no mayor a 3 meses). Se debe verificar que no haya usuarios con privilegios sin previa autorización.

3.5. CAMBIO DE ESTADO O FINALIZACIÓN DE UN CONTRATO

- El cambio a una posición diferente, dentro de la organización, debe ser reflejada en el retiro de todos los derechos de acceso que no fueron aprobados para esa nueva posición.
- Al dejar de ocupar, un trabajador, alguna posición ya sea por cambio de puesto o retiro de la empresa todos los derechos de acceso deben ser removidos o adaptados, incluyendo acceso físico y lógico, llaves, tarjetas de identificación, instalaciones del proceso de información, subscripciones y retiro de cualquier documentación que lo identifique como un miembro actual, del puesto o de la organización según corresponda.

3.6. GESTIÓN DE LA CLAVE DE USUARIO

Las contraseñas constituyen uno de los principales medios de validación de la autoridad de un usuario para acceder a un activo informático. Los sistemas de administración de contraseñas deben constituir una herramienta eficaz e interactiva que garantice contraseñas de calidad.

El sistema de administración de contraseñas debe:

- Imponer el uso de contraseñas individuales para determinar responsabilidades.
- Permitir que los usuarios seleccionen y cambien sus propias contraseñas (luego de cumplido el plazo mínimo de mantenimiento de las mismas) e incluir un procedimiento de confirmación para contemplar los errores de ingreso.
- Imponer una selección de contraseñas de calidad según lo señalado en el punto 3.1 “LINEAMIENTOS PARA EL PERFIL DE LOS USUARIOS”.
- Obligar a los usuarios a cambiar las contraseñas provisorias en su primer procedimiento de identificación, en los casos en que ellos seleccionen sus contraseñas.
- Enmascarar las contraseñas en pantalla, cuando son ingresadas.
- Almacenar en forma separada los archivos de contraseñas y los datos de sistemas de aplicación.
- Almacenar las contraseñas en forma cifrada utilizando un algoritmo de cifrado unidireccional.
- Modificar todas las contraseñas predeterminadas por el vendedor, una vez instalado el software y el hardware (por ejemplo, claves de impresoras, switchs, routers, etc.).
- Garantizar que el medio utilizado para acceder/utilizar el sistema de contraseñas, asegure que no se tenga acceso a información temporal o en tránsito de forma no protegida.

3.7. INSTALACIONES DE ACCESO RESTRINGIDO

Esta política define a continuación las instalaciones físicas que representan, en caso de visitas no deseadas o un bajo control de acceso un riesgo relevante para la seguridad de la información y, por lo tanto, deben ser de acceso restringido.

- **Área para Desarrollo**: Se considera como un espacio físico restringido debido a que en este espacio se maneja detalles de los proyectos y nuestro secreto industrial consistente en el código de las aplicaciones con los que brindamos nuestros servicios.
- **Data Center**: Ubicado al fondo de la oficina de DACTA, este espacio contiene los servidores que permiten almacenar y procesar toda la información que permiten a la organización brindar todos los servicios de su core de negocios.
- **Área destinada a Testing y Soporte al usuario**: Ubicado al costado del espacio que ocupa personal de Desarrollo en este espacio se maneja información confidencial de DACTA y de los clientes de DACTA.
- **Comercial**: Ubicadas en la parte frontal de la oficina del piso 2 del edificio, en este espacio se maneja información de contactos, potenciales clientes y nuevos proyectos de ventas y marketing por tanto el acceso de cualquier persona que no pertenezca a esta área está restringida. En caso de ausencia del personal esta oficina se debe cerrar con llave.
- **Finanzas y Contabilidad**: Ubicadas en el piso 2 del edificio y al costado de la oficina de Comercialización, esta otra oficina alberga información financiera relevante para la continuidad operativa de la institución a la cual debe restringirse el acceso para cualquier persona que no pertenezca a esta área.

3.8. ACCESOS AL DATACENTER

Acceso a la sala de máquinas

- El Coordinador de TI está encargado de hacer cumplir estas políticas.
- El acceso a la sala de equipos está permitido únicamente a personal Soporte de TI.
- El acceso de personal interno o externo a DACTA está restringida y únicamente podrán ingresar en compañía de personal de TI.
- Cada vez que alguien entre a la sala de máquinas debe quedar registrado, detallando: Nombre de la persona, DNI, empresa, motivo del ingreso, fecha y hora del ingreso y egreso.

Durante su permanencia debe estar siempre acompañado por personal debidamente autorizado.

Registro del Acceso de Personal Interno o Personal Externo

El acceso de personal interno o personal externo, autorizados a ingresar a las áreas restringidas debe quedar registrado, detallando nombre, DNI, empresa, motivo del ingreso, fecha y hora del ingreso y egreso.

Señalización

La ubicación de los equipos de Producción, no debe ser anunciada mediante signos o señales visibles o entendibles para cualquier persona.

3.9. TRASLADO DE EQUIPOS

Todo traslado de equipos de computación o de comunicaciones debe estar autorizado por el Coordinador de TI o en quien éste delegue dicha responsabilidad, debe ser efectuado por el personal de Soporte Interno y se debe informar al responsable para la actualización del inventario, dicho evento, debe identificar al menos, la persona, el equipo trasladado y los lugares de origen y destino.

Los equipos ingresados en forma temporal por terceros deben ser anotados en un registro para su control de entrada, salida, tiempo y usuario. Estos no podrán ser conectados a la red de DACTA.

Antes de que un equipo computacional sea vendido, donado o dado de baja, debe ser examinado por el Soporte de TI y proceder a la eliminación de toda información.

En caso de no cumplir con la presente Política Específica de Gestión de Accesos, los lineamientos de seguridad de la información u otros directivas o procedimientos de seguridad de la información, se reportará el evento al Oficial de Seguridad de Información para que tome conocimiento y disponga las acciones correspondientes, de considerarlo necesario. De esta forma, la autoridad competente de DACTA, tomará las medidas disciplinarias necesarias, las cuales están sujetas a la normativa vigente de DACTA.

4. AUDITORÍA

- El Oficial de Seguridad de la Información de DACTA se encargará de realizar la revisión de este control trimestralmente.
- Específicamente se revisará el registro con los privilegios de accesos a los datos personales.

5. REGISTROS

Código	Nombre de Registro	Responsable del Control	Tiempo de Conservación
F-E-SIG-003	Altas, bajas y modificaciones de usuarios con perfil general	Coordinador TI	12 meses
F-E-SIG-004	Altas, bajas y modificaciones de usuarios con acceso privilegiado	Coordinador TI	12 meses
F-E-SIG-005	Autorizaciones de acceso lógico (*)	Coordinador TI	12 meses
F-E-SIG-006	Revisión de los derechos de acceso lógico	Coordinador TI	12 meses
F-E-SIG-007	Ficha de ingreso de recursos informáticos externos	Coordinador TI	12 meses

6. CONTROL DE CAMBIOS

Versión	Fecha	Descripción	Elaborado por	Revisado por	Aprobado por
1	30/06/2021	Emisión	OSI	Comité SIG	Gerente General
2	20/09/2021	Actualización	OSI	Comité SIG	Gerente General
3	22/02/2023	Actualización	OSI	Comité SIG	Gerente General
4	22/02/2024	Revisión	OSI	Comité SIG	Gerente General
Firmas de la versión vigente			 S. Rafaile	 S. Rafaile	
			 A. Morales	 A. Morales	G. Rafaile

Identificación de las modificaciones	
Versión	**Descripción de cambios**
2	• Cambios varios en los capítulos 3.1 LINEAMIENTOS PARA EL PERFIL DE LOS USUARIOS • Cambios varios en: 3.2 LINEAMIENTOS PARA LOS USUARIOS DE PERFIL CON PRIVILEGIOS ESPECIALES • Cambios varios en: 3.2 GESTIÓN DE PRIVILEGIOS • Retiro de texto: Imponer cambios en las contraseñas en aquellos casos en que los usuarios mantengan sus propias contraseñas, según lo señalado en el punto 3.1 “LINEAMIENTOS PARA EL PERFIL DE LOS USUARIOS”.

	• Retiro del texto: “Revisar las asignaciones de privilegios a intervalos regulares (recomendable no mayor a 6 meses), a fin de garantizar que no se obtengan privilegios no autorizados”..
3	Se actualizó el documento con el nuevo logo de DACTA. Se actualiza el requisito normativo según nueva versión ISO 27001:2022.
4	Se modificó: 3.6 GESTIÓN DE LA CLAVE DE USUARIO Se utilizó el término “Enmascarar” para alinear la política con la norma ISO 27001:2022