

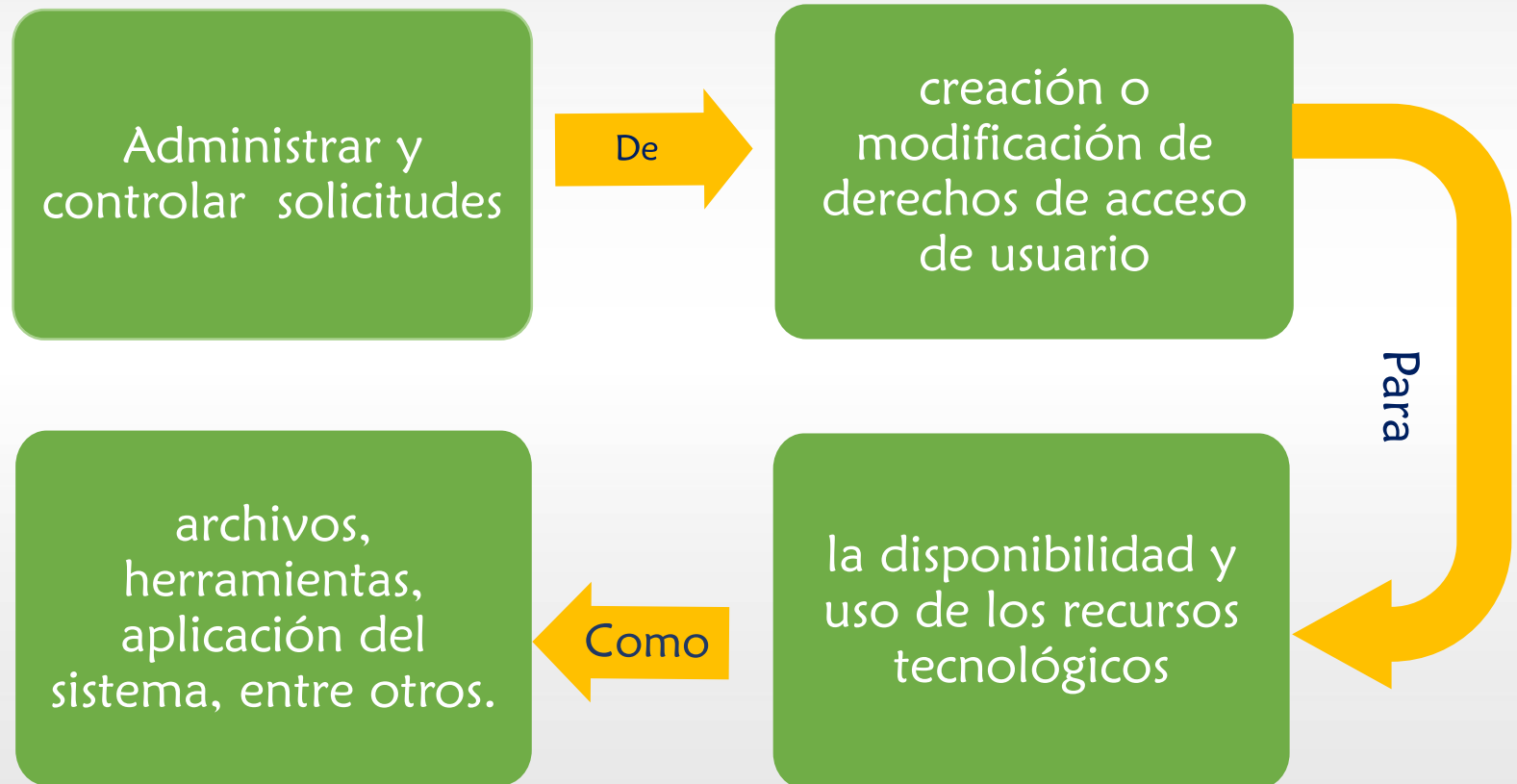


www.oasiscom.com

Procedimiento de Accesos y Permisos

Norma ISO/IEC 27001: 2013

1. Objetivo



2. Responsables



- ✓ Miguel Carvajal
- ✓ Lorena Padilla
- ✓ Fredy Prieto
- ✓ Jhonier Fino
- ✓ Maira Gutiérrez

**Equipo de Seguridad de la
Información**

3. Política de Control de Acceso

Acceso Físico



Todos los empleados de OasisCom deben tener registrada su huella dactilar.



El ingreso a las áreas seguras está habilitado sólo para las personas que la compañía designe.



Toda persona externa a OasisCom debe registrar su entrada en la recepción, permanecer siempre acompañado y portar el carné de visitante en un lugar visible.



Responsables de acceso a las instalaciones

Llaves y clave de acceso

Llave personal y clave

- | | |
|----------------------|------------------|
| ✓ Martín Gutiérrez | ✓ Eduardo Riaño |
| ✓ Margarita Ramírez | ✓ Lorena Padilla |
| ✓ Fernando Gutiérrez | ✓ Luisa Lozano |
| ✓ Miguel Carvajal | ✓ Sarina Moreno |
| ✓ Miguel Riaño | ✓ Victor Guerra |
| ✓ Angélica Ramírez | ✓ Andrés Bernal |

Llave compartida y clave

Soporte:

- ✓ Julián Garzón
- ✓ Cristhian Mayorga
- ✓ Rodrigo Ortíz
- ✓ Juan Fajardo

Administración

- ✓ Elvira Arias
- ✓ Andrés Castañeda

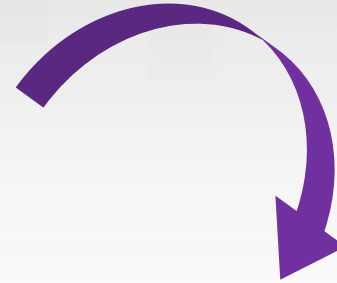
En caso de que un empleado permanezca en la oficina después del horario laboral, se debe asegurar que algún responsable principal o secundario se encuentre en las instalaciones para poder realizar el respectivo cierre



Proceso de aprobación para asignación de llave de la oficina – acceso físico



El Gerente de área debe enviar un correo al Gerente Administrativo justificando la asignación de llave que requiere hacer a uno de sus colaboradores.



Si la solicitud es aprobada por el Gerente Administrativo, este debe comunicar la decisión al gerente de área y debe hacer entrega de la llave y clave de seguridad al colaborador indicado en la solicitud.



Se debe incluir en el formato de Acta de Entrega de Puesto de Trabajo del colaborador, el número de llave asignada.



3. Política de control de acceso

Cuarto de Archivo

- ✓ **Responsable:**
Andrés Castañeda.
- ✓ **Autorizados:**
Integrantes del
proceso de
administración,
RRHH y mercadeo.

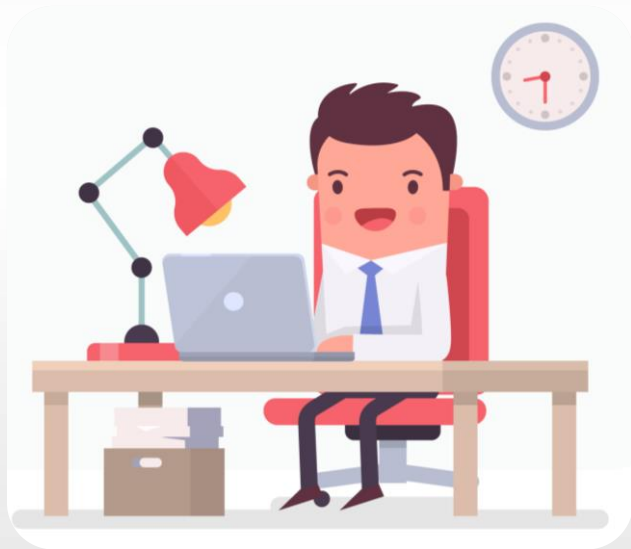
Áreas Seguras

Cuarto de Servidores

- ✓ **Responsable:**
Miguel Carvajal
- ✓ **Autorizados:**
Gestor Soporte
Nivel 1

ÁREAS RESTRINGIDAS

Puestos de trabajo

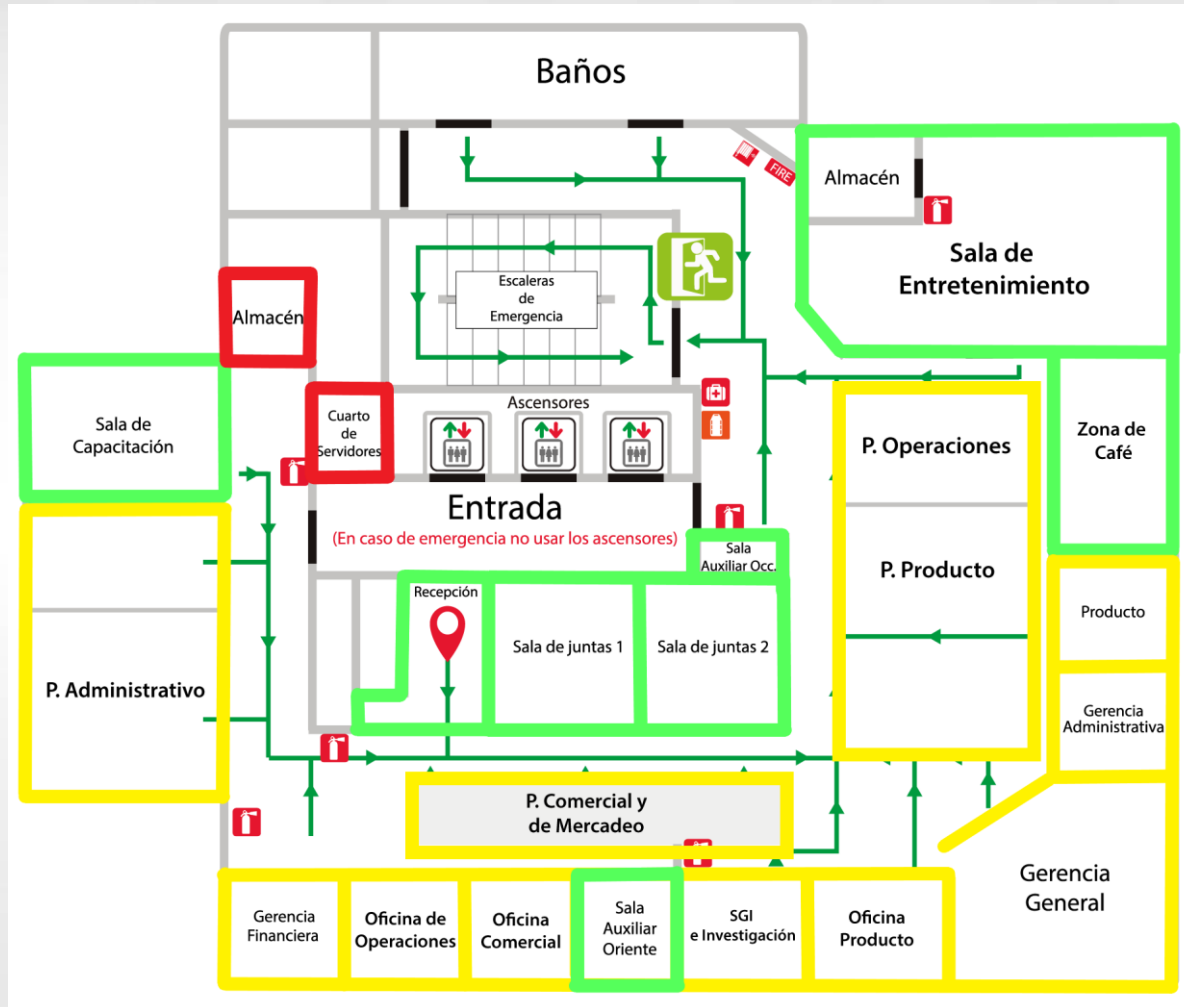


ÁREAS SOCIALES

- Salas de juntas y de capacitación
- Sala de entretenimiento
- Zona del café
- Recepción



3. Mapa áreas de OasisCom



3. Política de control de acceso

Acceso Lógico

El Gestor de Soporte Nivel 1 debe mantener actualizados los accesos y permisos de los roles de la empresa.



Si un colaborador de OasisCom cambia de cargo, se deben así mismo cambiar los permisos a las plataformas con base al nuevo cargo y asegurar que todos los permisos anteriores fueron retirados.



3. Política de control de acceso

Acceso a Plataformas



En el documento

*FO_SGSI_02_Formato_Matriz_
de_Accesos_y_Permisos* se definen los
roles y permisos de acceso para cada
una de las plataformas establecidas en la
organización.

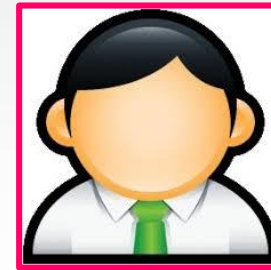
El **Director de Infraestructura** o el **Gestor
de Soporte Nivel 1** la actualizan o
modifican.

3. Política de control de acceso

Acceso a Computadores



Administrador



Estándar

Usuario con permiso total sobre la gestión del equipo, se establece contraseña general con conocimiento sólo del Director de Infraestructura y el Gestor de Soporte Nivel 1.

Usuario asignado al responsable del equipo para la gestión diaria, el responsable del equipo debe asignar una contraseña personal al dispositivo.

Solicitud o revocación de registro

La solicitud o revocación del registro de usuario en las diferentes plataformas de la empresa debe ser solicitado por el **Gestor de Contratación al Gestor de Soporte Nivel 1** cuando se inicie o termine el vínculo laboral con un colaborador de la organización.



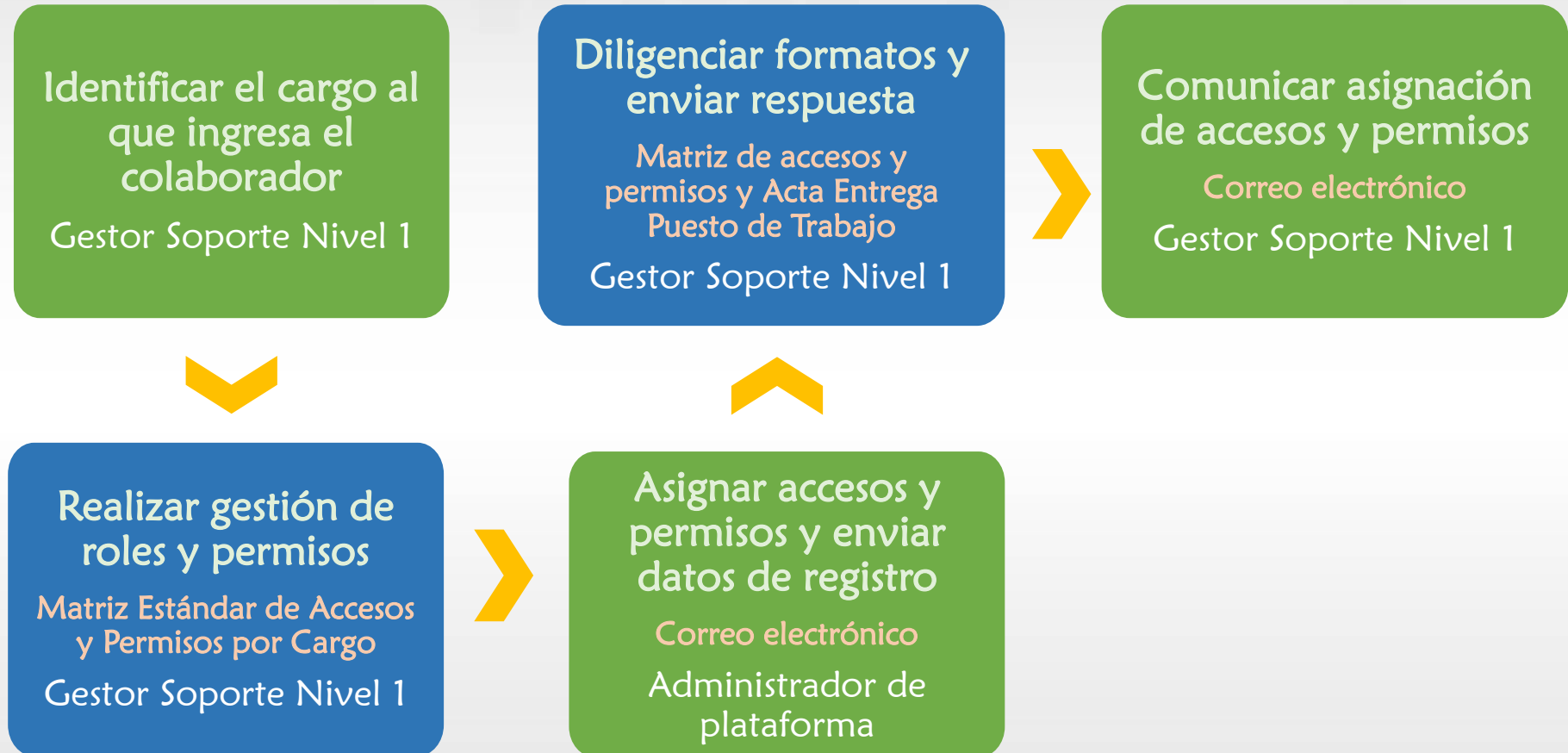
Basándose en el procedimiento
PR_GTH_06_Procedimiento_Ingreso_Retiro
_de_Empleados_y_Cambio_de_Cargo.

4. Matriz de Accesos y Permisos

La **Matriz de Accesos y Permisos** es un documento en el cual se consolidan los permisos de todos los colaboradores de OasisCom, esta es alimentada por el área de Infraestructura.

La **Matriz Estándar de Accesos y Permisos por Cargo** define por cada cargo los permisos estándar o mínimos que requiere para sus funciones. El Gestor de Soporte Nivel 1 podrá consultar con el gerente de área si el colaborador necesita un permiso o acceso adicional a lo definido.

5. Procedimiento de solicitud o cambio de accesos y permisos en plataformas



Ref. Matriz estándar de accesos y permisos por cargo

6. Procedimiento de eliminación de accesos y permisos en plataformas

Gestionar la revocación de accesos y permisos en plataformas

Gestor Soporte Nivel 1

Procedimiento_Ingreso_Retiro
_de_Empleados_y_Cambio_de_Cargo



Eliminar accesos y permisos

Administrador de plataforma

Matriz_de_Accesos_y_Permisos.
Email



Diligenciar acta de entrega

Gestor Soporte Nivel 1

Acta_Entregade_Puesto_de_Trabajo



Revisar activos

Director de infraestructura

Email


7. Permisos en plataformas OASISCOM y OASISKB

El colaborador debe enviar un correo electrónico al gerente de su área solicitando aprobación de acceso a la *aplicación* requerida o *carpeta (archivos)* con la *justificación* y por cuánto *tiempo* con copia a lorena.padilla@oasiscom.com, quien dará el acceso en caso de ser aprobado.



7. Permisos en plataformas

Los permisos deben ser aprobados y asignados por el responsable de cada plataforma



**Teniendo
en cuenta**

las características de clasificación de la información contenida o desarrollada en cada plataforma

7. Permisos en plataformas

Responsables

**Gestor de
Permisos**
(Lorena Padilla)



- ✓ OasisCom
- ✓ OasisKB
- ✓ Office 365
- ✓ OasisU

**Gerencia
Administrativa**
(Fernando
Gutiérrez)



- ✓ Colviseg
(Seguridad)

**Oficial de
Seguridad de la
Información**
(Miguel Carvajal)



- ✓ Bases de Datos
- ✓ Azure
- ✓ Telefonía e Internet
- ✓ Servidor de Archivos
- ✓ Redes
- ✓ Team Foundation
- ✓ Otras plataformas

8. Acceso a Redes y Servicio de Red



El personal de OasisCom tiene acceso a 2 redes tipo inalámbricas y 1 red tipo alámbrica para el correcto desarrollo de sus actividades y funciones dentro de la organización.

Se controla a través del firewall interno basándose en los permisos definidos en la Matriz de Accesos y Permisos

8. Acceso a Redes y Servicio de Red

Red Alámbrica

- Uso interno.
- Restricciones según el rol.

Red Inalámbrica Empleados

- Uso interno.
- Restricciones según el rol.
- Control a través de clave de acceso, dirección.

Red Inalámbrica Invitados

- Público externo a OasisCom.
- Protegida por clave de acceso.
- Separada de la red inalámbrica empleados.

Características de una Contraseña Segura



- ✓ Su longitud debe ser de mínimo 8 caracteres
- ✓ Mínimo 1 carácter alfabético en mayúscula
- ✓ Mínimo 1 carácter alfabético en minúscula
- ✓ Mínimo 1 carácter numérico
- ✓ Se recomienda incluir mínimo 1 carácter especial

9. Sistema de Gestión de Contraseñas

Directrices de una Contraseña Segura

No utilizar contraseñas que sean únicamente palabras (Nombres, ciudades, palabras en otro idioma)

Cada contraseña es de uso personal e intransferible

No utilizar contraseñas completamente numérica (teléfono, fechas, número de identificación).

Se debería realizar cambio de contraseña al menos una vez al año



Se deben notificar inmediatamente al Oficial de Seguridad de la Información si sospechan que alguien ha obtenido acceso sin autorización a su cuenta

9. Sistema de Gestión de Contraseñas

Directrices de una Contraseña Segura

Deben utilizar contraseñas diferentes en cada uno de los sistemas a los cuales tengan acceso

No se deben almacenar las contraseñas en los equipos para acceso automático

No se deben almacenar contraseñas en formato legible, en computadores sin control de acceso o en otros sitios donde personas no autorizadas puedan descubrirlos y utilizarlos.



Las contraseñas que hayan sido usadas para el acceso a las plataformas no deben ser asignadas nuevamente.

9. Sistema de Gestión de Contraseñas

Directrices de una Contraseña Segura

Es una norma tácita de buen usuario no mirar el teclado mientras alguien teclea su contraseña.

El usuario es responsable por la custodia de su contraseña. Debe evitar en lo posible digitar la contraseña mientras alguna persona está observando lo que escribe en el teclado.



Las contraseñas se deben transferir siempre de forma segura evitando que terceros puedan tener acceso a ellas.

10. Derechos de Acceso Privilegiado

Cada una de las plataformas utilizadas en la organización tienen definido un rol de **acceso privilegiado**, estos usuarios están definidos en la *Matriz de Accesos y Permisos*.

Características para la asignación de accesos privilegiados:

- ✓ Competencias gerenciales
- ✓ Capacitación en la utilización de la plataforma
- ✓ Tiempo en la organización
- ✓ Formación en carreras afines a ingeniería y conocimientos sobre el SGSI.

11. Gestión y Uso de la autenticación secreta

Cuando se solicite el cambio de contraseña por correo, el responsable de cada plataforma debe contactar a quien solicita el cambio y verificar su identidad antes de realizar la asignación de la nueva contraseña de acceso.



11. Gestión y Uso de la autenticación secreta

Reestablecer contraseña

Los colaboradores lo pueden hacer directamente desde <https://portal.office365.com>.

Si se solicita al administrador de la plataforma, se debe proporcionar un e-mail alternativo para el envío de la contraseña.

Se debe confirmar por e-mail el recibido de la contraseña al administrador de la plataforma.




✓ <https://app.oasiscom.com/>

- ✓ Máximo **3** intentos de inicio de sesión antes de **deshabilitar el usuario**.
- ✓ Para **habilitar el usuario**, se debe enviar por e-mail la solicitud al administrador de la plataforma.

12. Ingreso seguro

 **Office** <https://mail.oasiscom.com>

 **OasisKB** <https://oasiskb.oasiscom.com>

 **OasisU** <http://oasisu.oasiscom.com>

 **OasisCom**
Cloud Solutions <https://app.oasiscom.com>

13. Uso de programas utilitarios privilegiados

La instalación de aplicaciones utilitarias
está a cargo del **Director de
Infraestructura** o **Gestor de Soporte
Nivel 1** con previa autorización del
Oficial de Seguridad de la Información.



El **Director de Infraestructura** o **Gestor de Soporte Nivel 1** harán
revisión semestral de los
programas instalados y
desinstalarán los que no hayan
sido autorizados por el **Oficial de
Seguridad de la Información**.

14. Control de acceso al Código Fuente

- ✓ Protección de acceso por medio de **Team Foundation Server**
 - ✓ **Team Foundation Server** lleva un historial de accesos y cambios en donde se identifica fecha y usuario responsable.
 - ✓ Los roles y usuarios autorizados en **Team Foundation Server** se definen en la matriz de accesos y permisos.
- ✓ Se realizan copias de seguridad de la plataforma **Team Foundation Server**



GRACIAS