CONTROL 11. SEGURIDAD FÍSICA Y DEL ENTORNO

NORMA ISO/IEC 27001:2013

OasisCom
Cloud Solutions

Tabla de contenido

Tabla de contenido

1. Áreas Seguras

Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.

OasisCom
Cloud Solutions

1.1. Perímetro de seguridad física

- ✓ La recepción del edificio donde se encuentra ubicado OasisCom, cuenta con la vigilancia de una empresa privada que se encarga de dar gestión al acceso de terceros, solicitando autorización previa de algún colaborador de la empresa.

- ✓ OasisCom cuenta con un biométrico a la entrada de la puerta principal para dar acceso a los colaboradores.

OasisCom
Cloud Solutions

1.1. Perímetro de seguridad física

- ✓ Con el botón que se encuentra ubicado en el escritorio de recepción se permite el ingreso a terceros y/o visitantes.
- ✓ Se cuenta con una alarma de seguridad para la protección de las instalaciones, la cual está bajo supervisión de una empresa privada de vigilancia.

OasisCom
Cloud Solutions

1.1. Perímetro de seguridad física

- ✓ Al hacer cierre de las instalaciones de OasisCom, los encargados de la llave y clave, deben activar la alarma con la clave y dejar la puerta con llave. Al ingresar, se debe desactivar la alarma.

- ✓ En caso de que la alarma se dispare o no sea activada, la empresa privada de vigilancia debe informar a los encargados de esta.

OasisCom
Cloud Solutions

1.2. Controles de acceso físicos

- ✓ Los visitantes que ingresen a las instalaciones de OasisCom deben registrar en la planilla de recepción *FO_GA_09_Formato_Control_de_Visitantes* la fecha y hora de ingreso y retiro.

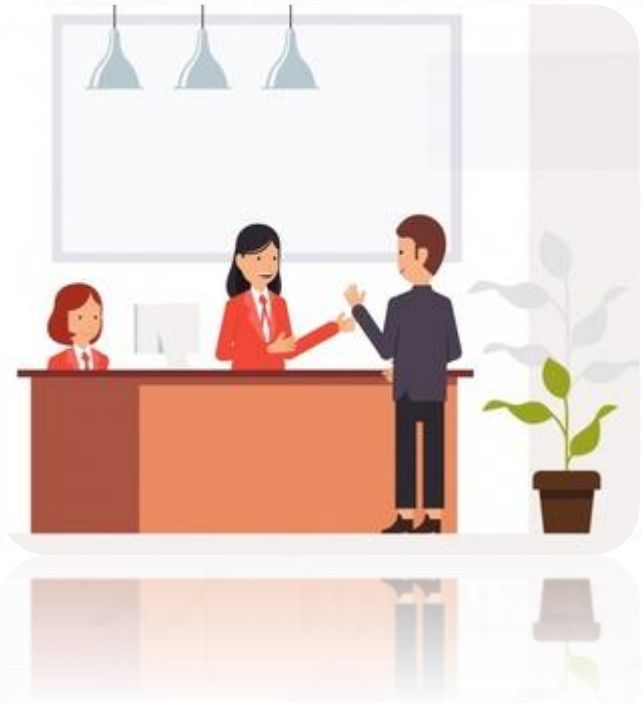
- ✓ La persona encargada de recepción debe entregarle a los visitantes el carné correspondiente, y estos deben portarlo en un lugar visible.

OasisCom
Cloud Solutions

1.2. Controles de acceso físico

- ✓ Tanto los visitantes como los colaboradores de OasisCom, deben portar el carné en un lugar visible.

- ✓ La persona encargada de recepción debe informarle el ingreso del visitante al colaborador encargado, quien debe recibirlo en recepción y siempre acompañarlo durante la estadía en las instalaciones de OasisCom.



OasisCom
Cloud Solutions

1.2. Controles de acceso físico

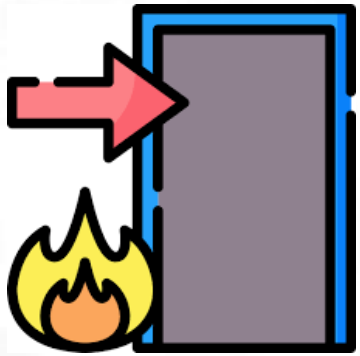
- ✓ En caso de identificar a un visitante sin el carné visible o sin acompañamiento, se le debe notificar al responsable de recepción o a un integrante del Equipo de Seguridad.
- ✓ Los accesos a las áreas seguras se deben revisar y actualizar de ser necesario.

OasisCom
Cloud Solutions

1.3. Seguridad de oficinas, recintos e instalaciones

Las instalaciones de OasisCom cuentan con cuatro puertas de ingreso:

- ✓ Una puerta de ingreso ubicada en la zona de las escaleras, catalogada para casos de emergencia, la cual sólo se habilita desde la parte interior de la empresa.



- ✓ Tres puertas ubicadas en la zona de los ascensores de las cuales sólo la puerta principal se encuentra habilitada para el ingreso.

OasisCom
Cloud Solutions

1.3. Seguridad de oficinas, recintos e instalaciones

- ✓ La puerta principal siempre debe estar cerrada para evitar el ingreso de personal no autorizado.

- ✓ Las dos puertas auxiliares de acceso a las instalaciones de OasisCom siempre deben estar cerradas a menos que exista autorización previa de Gerencia Administrativa.

OasisCom
Cloud Solutions

1.4. Protección contra amenazas externas y ambientales

- ✓ Con el fin de atender cualquier emergencia, OasisCom cuenta con una estructura que permita dar seguridad a los empleados, mejorar el nivel de seguridad empresarial, proteger bienes y activos; y ayudar al cumplimiento de las disposiciones legales vigentes.

OasisCom dispone de:

OasisCom Cloud Solutions

1.4. Protección contra amenazas externas y ambientales

- ✓ Una brigada de emergencias conformada por 10 funcionarios de la empresa.

- ✓ Nueve extintores portátiles distribuidos en las instalaciones.

- ✓ Unas rutas y salidas de evacuación.

- ✓ Un sistema de alarma para evacuación.

OasisCom Cloud Solutions

1.4. Protección contra amenazas externas y ambientales

- ✓ Un gabinete contra incendios en el piso, que contienen: manguera, hacha, extintor.

- ✓ Un botiquín y camilla con inmovilizadores de miembros superiores e inferiores ubicado al lado izquierdo de la puerta de escalera de emergencias para la atención de emergencias el cual contiene los elementos de atención básica para primeros auxilios.

OasisCom
Cloud Solutions

1.4. Protección contra amenazas externas y ambientales

- ✓ Una red hidráulica contraincendios con rociadores automáticos: distribuidos cada tres metros aproximadamente dentro de toda la oficina.

- ✓ Protocolos estándar en caso de sismo, explosión, terrorismo y/o fuga de gas.

OasisCom Cloud Solutions

1.4. Protección contra amenazas externas y ambientales

- ✓ Un Plan contraincendios.
- ✓ Contacto de servicios de apoyo (bomberos, grupos de socorro, entidades de apoyo, entidades de respuesta médica, hospitalaria y riesgos laborales y servicios de transporte).

1.4. Protección contra amenazas externas y ambientales

Proceso para contacto con autoridades y entidades sobre Seguridad de la Información:

- ✓ Los incidentes que sean categorizados como críticos, según el análisis realizado por el Oficial de Seguridad de la Información y las gerencias de la empresa, serán reportados según la instancia correspondiente a los siguientes contactos:

OasisCom
Cloud Solutions

1.4. Protección contra amenazas externas y ambientales

- ✓ Policía Nacional de Colombia
- ✓ Fiscalía General de la Nación
- ✓ MinTIC
- ✓ Claro
- ✓ Une
- ✓ Azure
- ✓ Microsoft

Para más información consulte el documento *OR_SIG_08_Plan_de_Emergencias.*

OasisCom Cloud Solutions

1.4. Protección contra amenazas externas y ambientales

- ✓ El edificio donde se encuentra ubicado OasisCom cuenta con un Comité de Emergencias el cual está conformado por personas del Edificio, entre ellos los brigadistas de OASISCOM, quienes se encargan de crear, planear y administrar el plan de emergencias.

OasisCom
Cloud Solutions

1.4. Protección contra amenazas y ambientales

Para garantizar la seguridad de la información y de los equipos de la empresa, se debe:

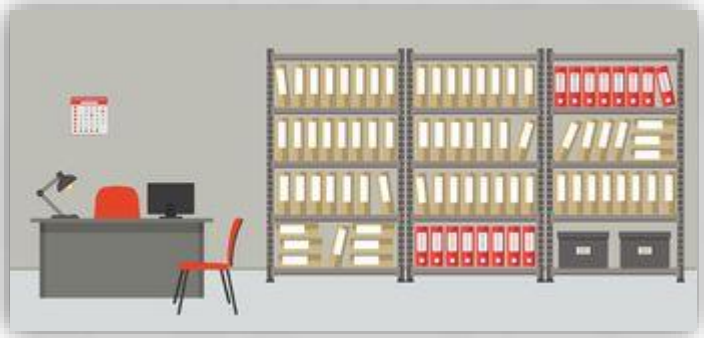
- ✓ Definir en las áreas responsabilidades para protección de documentos que lo requieran, en caso de una evacuación.
- ✓ Asegurar las puertas de emergencia y de acceso a la oficina al finalizar la evacuación.

OasisCom
Cloud Solutions

1.5. Trabajo en áreas seguras

OasisCom define como áreas seguras dentro de las instalaciones de la empresa las siguientes:

Cuarto de archivo



Cuarto de servidores

La Gerencia Administrativa y Financiera cuenta con copia de la llave de las áreas seguras de OasisCom.

OasisCom
Cloud Solutions

1.5. Trabajo en áreas seguras

- ✓ Los colaboradores deben tener conciencia a cerca de cuáles son las áreas seguras.
- ✓ El ingreso a estas es exclusivo de sus responsables.
- ✓ El responsable del área segura o a quien este designe debe supervisar los trabajos realizados por los contratistas en el área segura a su cargo.

OasisCom
Cloud Solutions

1.5. Trabajo en áreas seguras

- ✓ Los contratistas que se encuentren en estas áreas deben permanecer en ellas y no desplazarse por otras sin supervisión del responsable.

- ✓ El responsable del área segura debe garantizar el correcto funcionamiento del control de acceso físico establecido para su área a cargo.

OasisCom
Cloud Solutions

1.5. Trabajo en áreas seguras

- ✓ Sólo los colaboradores y/o contratistas designados para hacer algún tipo de trabajo en ellas deben conocer de la gestión y controles que allí se deben seguir.

- ✓ El responsable del área segura o quién este delegue, debe proporcionar los requisitos de seguridad de su área en particular y garantizar su cumplimiento.

OasisCom
Cloud Solutions

1.5. Trabajo en áreas seguras

- ✓ El Oficial de Seguridad de la Información periódicamente debe hacer seguimiento al cumplimiento de los requisitos de seguridad definidos para las áreas seguras.

- ✓ Está prohibido hacer registro de video, fotografía o grabación a menos que se cuente con autorización previa del responsable del área segura para ello. Además, está prohibido comer, beber o fumar.

OasisCom
Cloud Solutions

1.5. Trabajo en áreas seguras

- ✓ Estas áreas deben estar etiquetadas con restricción de acceso y cerradas bajo llave cuando el responsable de esta o su designado no se encuentre en ella.

- ✓ Para el ingreso al cuarto de servidores se debe diligenciar el formato *FO_SGSI _01_Formato_Ingreso_y_Salida_Cuarto_ Servidores.*

OasisCom
Cloud Solutions

1.6. Área de despacho y carga: Recepción

- ✓ Quien atienda la solicitud de autorización de ingreso, debe validar con el colaborador a quien le traen la encomienda para autorizar el ingreso del personal de mensajería. Los paquetes de encomienda se deben registrar en el documento *FO_GA_08_Formato_Control_y_Seguimiento_ Correspondencia,* ubicado en recepción.

OasisCom
Cloud Solutions

1.6. Área de despacho y carga

- ✓ El personal que llega con paquetes de encomienda debe permanecer sólo en la zona de recepción y no desplazarse por otras áreas sin autorización. Los paquetes deben ser inspeccionados, asegurando que se encuentra en perfectas condiciones sin evidencia de alteración ni elementos extraños.

OasisCom
Cloud Solutions

1.6. Área de despacho y carga

Los portátiles que ingresen los visitantes a OasisCom deben ser registrados en el formato *FO_GA_09_Formato_control_de _visitantes ubicado en la recepción.*

OasisCom
Cloud Solutions

2. Equipos

Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.

OasisCom
Cloud Solutions

2.1. Ubicación y protección de los equipos

- ✓ Las áreas seguras deben estar protegidas del acceso de personal no autorizado.
- ✓ Los servidores y equipos de comunicación se deben resguardar en el área segura, instalados y almacenados en Racks cumpliendo con las condiciones eléctricas y ambientales debidas. El acceso al área debe ser controlado por el responsable.

OasisCom
Cloud Solutions

2.1. Ubicación y protección de los equipos

- ✓ Los puestos de trabajo del área financiera y contable deben estar ubicados en áreas que minimicen el riesgo de que personas no autorizadas puedan ver la información durante su uso.

OasisCom
Cloud Solutions

2.1. Ubicación y protección de los equipos

- ✓ A menos que haya autorización expresa o acompañamiento de un colaborador a un tercero, los equipos sólo deben ser operados por los colaboradores de OasisCom para evitar poner en riesgo la seguridad de la información.

OasisCom
Cloud Solutions

2.1. Ubicación y protección de los equipos

- ✓ Los colaboradores de OasisCom y/o Proveedores deben abstenerse de tener recipientes con líquidos o alimentos cerca de los equipos, que eventualmente puedan causar averías a los mismos.

- ✓ Se dispone de instalaciones con espacios adecuados (escritorios) para mantener los equipos en condiciones ambientales y de trabajo ideales según las especificaciones de los fabricantes.

OasisCom
Cloud Solutions

2.2. Servicios de suministro

Se dispone de:

- ✓ Conexiones reguladoras de suministro eléctrico con el fin de evitar daños a los equipos por posibles descargas eléctricas.

- ✓ Una UPS, para respaldar el suministro eléctrico a los servidores y equipos de comunicaciones de la compañía.

- ✓ Dos canales de comunicación (Servicio de Internet) operando simultáneamente para así asegurar una disponibilidad constante de dicho servicio.

OasisCom
Cloud Solutions

2.2. Servicio de suministro

OasisCom debe evaluar periódicamente la eficiencia de estas medidas para comprobar su eficacia y plantear medidas de mantenimiento o actualización para asegurar la disponibilidad de los servicios eléctricos y de comunicaciones.

OasisCom Cloud Solutions

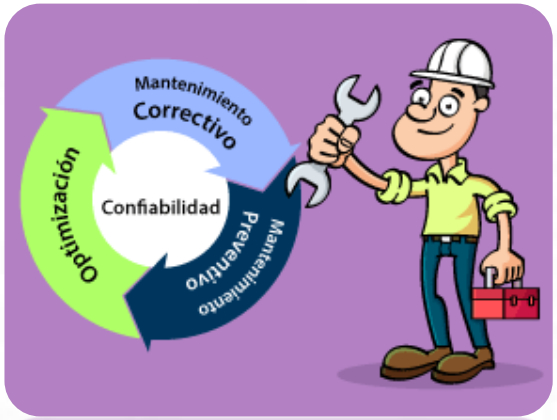
2.3. Mantenimiento de equipos

OasisCom define en el procedimiento de gestión de mantenimiento los lineamientos para asegurar la disponibilidad e integridad continua de sus activos de información:

- ✓ A la UPS se le debe hacer un mantenimiento preventivo cada 6 meses.
- ✓ Al menos una vez al año, o en menos tiempo según corresponda, se le debe hacer mantenimiento preventivo a todos los equipos de OasisCom.

OasisCom
Cloud Solutions

2.3. Mantenimiento de equipos



- ✓ En el documento *FO_SS_03_Inventario_Hardware_Software_OasisCom* se define el plan de mantenimiento preventivo.
- ✓ En el documento *FO_SS_03_Inventario_Hardware_Software_OasisCom* se definen las actividades básicas que se deben realizar en los mantenimientos por cada tipo de activo.

OasisCom
Cloud Solutions

2.4. Retiro de activos

Los gerentes, el personal de Proyectos, Soporte y Comercial, están autorizados para retirar su equipo de cómputo cuando lo requieran para el desarrollo de sus actividades. A excepción de los gerentes, al retirar el equipo se debe registrar en el formato FO_GA_10_Formato_Control_de_Retiro_de_Activos.

OasisCom
Cloud Solutions

2.4. Retiro de activos

Para los colaboradores de las demás áreas que requieran retirar su equipo u otro activo, el gerente de área debe enviar un correo al Director de Infraestructura autorizando el retiro del equipo, donde especifique nombre del colaborador, número de activo del equipo que retira y el tiempo estimado de ausencia.

OasisCom
Cloud Solutions

2.4. Retiro de activos

- ✓ Todo activo que se retire, se debe registrar en el documento *FO_GA_10_ Formato_Control_de_Retiro_de_Activos* ubicado en la recepción. Una vez se regrese el activo, se debe actualizar la planilla con la fecha y hora de ingreso y hacer su respectiva devolución al responsable del activo.

- ✓ OasisCom debe capacitar al personal sobre la seguridad de los activos en el retiro de los mismos de la oficina.

OasisCom
Cloud Solutions

2.5. Seguridad de equipos y activos fuera de las instalaciones

- ✓ Los activos retirados de las oficinas que se usen en lugares públicos nunca deben ser desatendidos para evitar cualquier inconveniente con los mismos

- ✓ Los activos retirados de las oficinas se deben transportar en los medios adecuados y ser usados bajo condiciones adecuadas para preservar su correcto funcionamiento, ya sea maleta, caja o cualquier otro que el fabricante estipule.

OasisCom
Cloud Solutions

2.5. Seguridad de equipos y activos fuera de las instalaciones

- ✓ Para los equipos de cómputo, se hace necesario conectarse solo a redes de confianza, asegurando que el antivirus y/o Firewall siempre estén activos. Adicionalmente, para aquellos activos que lo permitan, se debe contar con una contraseña para acceder a ellos.

OasisCom
Cloud Solutions

2.6. Disposición segura o reutilización de equipos

- ✓ Se debe hacer copia de seguridad de respaldo de los activos que se vayan a disponer con el fin de no perder información que pueda ser de importancia para la empresa.

- ✓ Los equipos que cuenten con medios de almacenamiento deben ser formateados profundamente para asegurar que información sensible no quede almacenada en ellos, antes de volverlos a usar y/o reasignar dicho equipo.

OasisCom
Cloud Solutions

2.6. Disposición segura o reutilización de equipos

- ✓ En caso de una falla crítica de un equipo, se debe borrar la información contenida en el medio extraíble o ser destruido en caso de que dicho medio también presente fallas. Con la disposición del equipo, se debe eliminar dicho equipo en el documento *FO_SS_03 _Inventario_ Hardware_Software_ OasisCom*.

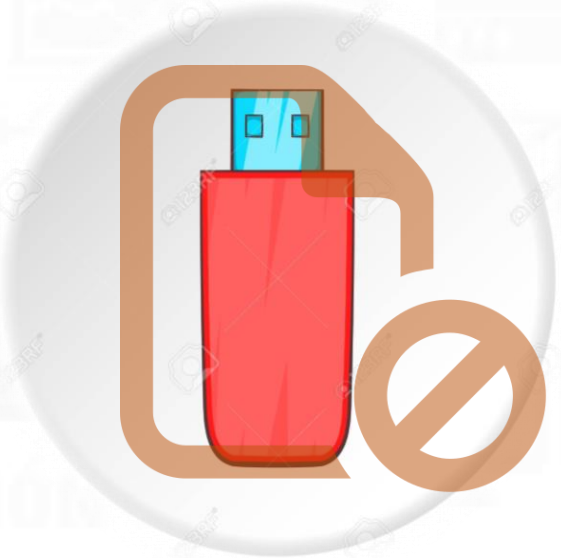
Para la disposición correcta se debe contactar a un proveedor.

OasisCom Cloud Solutions

2.6. Disposición segura o reutilización de equipos

- ✓ Los dispositivos de almacenamiento removible con que cuenta la compañía se deben formatear una vez al mes, para asegurar que información sensible no esté contenida en ellos.

- ✓ Si el activo a disponer se encuentra registrado en el módulo de activos fijos de la compañía se debe seguir el *PR_GA_06_Procedimiento_Gestión_Activos.*



OasisCom
Cloud Solutions

2.7. Equipos de usuario desatendidos

Prácticas al dejar desatendido su equipo:

- ✓ Bloquear la sesión del computador (Windows + L) siempre en los momentos que se vaya a ausentar del puesto de trabajo.

- ✓ Los equipos deben tener configurado el bloqueo de sesión automático después de 3 minutos de inactividad.

OasisCom
Cloud Solutions

2.7. Equipos de usuario desatendidos

- ✓ En equipos servidores se debe desactivar (log off) la sesión si se pretende apagar el equipo o si simplemente se va a dejar desatendido por un periodo de tiempo considerable.

- ✓ Al retirarse del puesto, se debe verificar que no quede información "Restringida" expuesta que utilicen para el desarrollo de sus labores, asegurando en forma apropiada dicha información.

OasisCom
Cloud Solutions

2.8. Política de escritorio limpio y pantalla limpia

OasisCom adopta una política de escritorios limpios para papeles, y medios de información, junto con una política de pantalla limpia, con el fin de reducir los riesgos por pérdida, daño a la información durante o fuera de las horas de trabajo.

OasisCom
Cloud Solutions

2.8. Política de escritorio limpio y pantalla limpia

- ✓ Papeles y medios de información deben estar asegurados en escritorios o archivadores especiales, principalmente en horas fuera de las normales de trabajo.

- ✓ Información física confidencial y crítica para la organización como lo son contratos, debe ser asegurada preferiblemente en archivadores resistentes a impacto, fuego e inundación.

OasisCom
Cloud Solutions

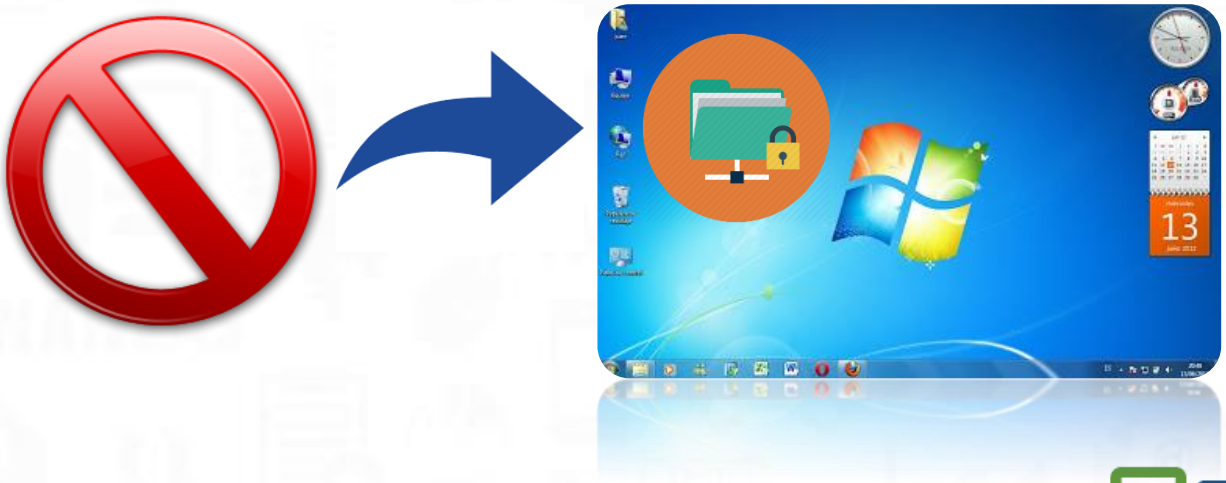
2.8. Política de escritorio limpio y pantalla limpia

- ✓ Los equipos no se deben dejar en sesión activa cuando no estén en uso o se ausenten del puesto de trabajo. Se recomiendo el uso de contraseñas y otro tipo de controles.

OasisCom
Cloud Solutions

2.8. Política de escritorio limpio y pantalla limpia

- ✓ Los escritorios de los equipos no deben contener información digital “confidencial” o “sensible” para la empresa expuesta que pueda ser vulnerable a robo, daño o acceso no autorizado. El escritorio solo debe contar con los accesos directos a las aplicaciones más usadas por el trabajador.



OasisCom
Cloud Solutions


OasisCom
Cloud Solutions
You
Tube