GOBIERNO DE SAN JUAN | MINISTERIO DE HACIENDA Y FINANZAS | DIRECCIÓN DE CIBERSEGURIDAD

Políticas de acceso al Centro de Datos y Procedimientos

Contenido

Introducción 2

Política y procedimiento de seguridad física del centro de datos 2

Descripción general 2

Directrices primarias 2

Niveles de acceso al centro de datos. 2

Acceso general. 2

Acceso acompañado. 3

Acceso limitado. 3

Puerta del centro de datos 3

Informe de excepciones 4

Solicitud/revocación de acceso al Centro de Datos 4

Políticas generales de operaciones del Centro de Datos para Área/Proyectos 4

Política general de alojamiento para la planificación de la capacidad del Centro de Datos 4

-Datos de Compra- 5

-Datos Instalación- 5

Política general sobre el trabajo de infraestructura en el Centro de Datos 5

Política general de seguridad 5

Política general de limpieza. 5

Introducción

Los procedimientos descritos en este documento han sido desarrollados para mantener un entorno de Centro de Datos seguro y limpio, debe ser seguido y respetado por personas que trabajan en el mismo. Es importante que cualquier área/proyecto que contemple el alojamiento de sus servidores en el Centro de Datos comprenda completamente y acepte los términos detallados a continuación.

Política y procedimiento de seguridad física del centro de datos

Descripción general

La seguridad del Centro de Datos es responsabilidad de la Secretaria de la Gestión Pública, dependiente del Ministerio de Hacienda y Finanzas. La misma es la encargada de definir las políticas de seguridad y posterior auditoria de estas, así también los principales participes en las operaciones que involucren al Centro de Datos.

Es importante que todo personal del Gobierno de San Juan respete estas políticas y prácticas, las cuales rigen el acceso a esta área sensible. En caso de no seguirlas se podrán aplicar medidas disciplinarias al personal.

Directrices primarias

El Centro de Datos es un área restringida que requiere un nivel de control alto, mayor que los espacios normales de la Administración Pública. Solo aquellos individuos quienes estén expresamente autorizados podrán ingresar a la misma. Los privilegios se otorgan a las personas que tienen una necesidad operativa legítima dentro del Centro de Datos. Además, esta área puede ser accedida sólo para realizar tareas de mantenimiento o instalaciones específicas.

Cualquier pregunta con respecto a las políticas y procedimientos debe ser abordada con la Direcciónde Ciberseguridad, perteneciente a la Subsecretaria de Infraestructura Tecnológica (SIT).

La única excepción permitida de las políticas y las prácticas de seguridad del Centro de Datos, son la suspensión temporal de estas reglas si es necesario proporcionar acceso de emergencia a médicos, bomberos, policías, etc.

Niveles de acceso al centro de datos.

Hay 3 “Niveles de acceso” al Centro de datos - **acceso general, acceso escoltado y acceso limitado.**

Acceso general.

Otorgado a las personas que tienen autoridad de acceso libre en el centro de datos.

Se concede acceso general a personal cuyas responsabilidades laborales requieren que tengan acceso al Centro de Datos. En primeras instancia personal perteneciente a la Secretaría de la Gestión Pública.

Acceso acompañado.

Es un acceso supervisando de cerca a las personas que tienen una necesidad operativa legítima de acceso infrecuente al Centro de Datos.

"Acceso Infrecuente" se define generalmente como el acceso requerido por un tiempo definido y limitado.

A las personas con acceso acompañado no se les otorgará una tarjeta para acceder al centro de datos.

El acceso escoltado a una persona que recibe acceso al área debe registrarse y documentarse, así como también debeser supervisión por una persona con acceso general, proporcionando una identificación positiva, y abandonando el área cuando se le solicite hacerlo.

Acceso limitado.

Se otorga a una persona que no califica para el acceso general, pero tiene una razón operativa legítima para el acceso no supervisado dentro del Centro de Datos.

Las personas con acceso limitado recibirán una tarjeta con acceso temporal al Centro de Datos, una vez debidamente autorizado serán escoltados al Centro de Datos dándoles acceso y explicándoles el protocolo.

El personal de acceso limitado solo puede entregar accesos acompañado a individuos relacionados con la operación vigente. El otorgante es responsable de estos individuos y debe escoltarlos al Centro de Datos cada vez que deseen entrar, estando en conocimiento de día y horarios de accesos.

Puerta del centro de datos

Todas las puertas del Centro de Datos deben permanecer cerradas en todo momento y solo pueden abrirse temporalmente por períodos que no deben exceder lo mínimo necesario para:

- Permitir la entrada y salida autorizada y registrada de individuos autorizados.
- Permitir la transferencia de suministros/equipos supervisados directamente por una persona que tenga acceso general a la zona.
- Abrir la puerta del Centro de datos SOLAMENTE si es necesario aumentar el flujo de aire en el centro de datos en el caso de un fallo del aire acondicionado. En este caso, el personal con acceso general debe estar presente y limitar el acceso al Centro de Datos.

Informe de excepciones

Todas las infracciones de las políticas y procedimientos de seguridad física del Centro de Datos deben ser informadas inmediatamente a la Dirección de Ciberseguridad. Si está justificado (por ejemplo: peligro de emergencia, inminente, etc.) la Dirección de Control Operativo debe ser notificada tan pronto como sea razonablemente posible.

Cuando se encuentra una persona no autorizada en el Centro de Datos, se debe informar inmediatamente a cualquier miembro de la Dirección de Ciberseguridad. Si esto ocurre durante horario fuera del laboral, un directivo de la dirección es el que debe ser contactado. Ellos determinarán las acciones a seguir.

La persona no autorizada debe ser escoltada desde el Centro de Datos y generar un informe escrito, el cual debe enviarse de inmediato a la Dirección de Ciberseguridad.

Las personas con acceso general al área deben monitorearla y sacar cualquier persona que parezca estar comprometiendo la seguridad, sus actividades, o estar interrumpiendo la operación normal del mismo. Es particularmente importante que individuos con acceso general muestren iniciativa para monitorear y mantener la seguridad del Centro de Datos.

Solicitud/revocación de acceso al Centro de Datos

Las áreas/proyectos que tengan equipo de computación en el Centro de Datos pueden solicitar acceso al mismo. Las personas designadas por el solicitante, el área/proyecto, tendrá acceso una vez que la Dirección de Ciberseguridad los autorice.

Una vez aprobado por un directivo de la Dirección de Ciberseguridad, el personal de la dirección creará una cita con la persona que solicita el acceso para proporcionarle a la personauna copia de las políticas de acceso al Centro de Datos.

Cuando una persona que tiene acceso al Centro de Datos termina su empleo o es transferido fuera del área, dicha área deberá notificar el evento a la Dirección de Ciberseguridad de forma fehaciente e inmediata para que el acceso de la personal a Centro de Datos sea revocado.

Políticas generales de operaciones del Centro de Datos para Área/Proyectos

Política general de alojamiento para la planificación de la capacidad del Centro de Datos

Cualquier instalación de equipamiento nuevo en el Centro de Datos debe ser consultada a la Dirección de Ciberseguridad, al momento de la toma de la decisión y lo antes posible (preferiblemente meses antes de que se ordene el equipo físico), para que, previo a una evaluación y coordinación, la Dirección de Ciberseguridad confirme si el equipo puede ser alojado. Para ello el solicitante debe informar:

-Datos de Compra-

- Día de entrega previsto
- Número de pedido para el equipo (si se conoce)
- Nombre del vendedor y descripción del equipo.
- Persona a contactar cuando llegue el equipo.

-Datos Instalación-

- Fecha aproximada de la instalación.
- Proveedor u organismo encargado de la instalación y descripción y ubicación del equipo a instalar.
- Nombre del Directivo a ser notificado una vez que el equipo sea instalado.

Política general sobre el trabajo de infraestructura en el Centro de Datos.

Se debe notificar todo el trabajo a realizar relacionado con la infraestructura del Centro de Datos. Esto incluye cosas tales como la instalación/eliminación de equipos, construcción o cualquier actividad que agregue/elimine activos al Centro de Datos.

Cualquier trabajo realizado se debe documentar adecuadamente en el formulario de control de cambios, provisto por la Dirección de Ciberseguridad.

Política general de seguridad

Todos los individuos en el Centro de Datos deben realizar su trabajo con una previa autorización y coordinación de las áreas afectadas y aplicando todas las políticas relacionadas con la seguridad.

Política general de limpieza.

El Centro de Datos debe mantenerse lo más limpio posible. Luego de cada actividad que concurra en el mismo se debe controlar la limpieza, eliminando adecuadamente cajas, basura, etc. El personal debe cerciorarse de que las herramientas deben ser reubicadas a su lugar legítimo.

Comida y bebida están expresamente prohibidasen el Centro de Datos.