	Política de Seguridad Física del Data Center		Código: POL 2011 Rev. 4
			Fecha de vigencia: Según publicación
	Responsables de la ejecución: Jefatura de Seguridad Física,	Aplicación: Claro Argentina	Pag:1 de 7

I. OBJETIVO

Establecer y determinar el alcance de los cuatro aspectos de la seguridad física para nuestro Data Center Olleros, de modo a resguardar, proteger en primer término la vida humana y también evitar la pérdida, daño o interrupción de los equipamientos, medios de transmisión o sistemas de información que en su interior se resguardan y desarrollan.

II. ALCANCE

La siguiente Política aplica a todo el Data Center Olleros 2770 - Argentina.

La Seguridad Física es uno de los pilares del Data Center. Los aspectos a desarrollar son:

1. Las Barreras Físicas y Edilicias.
2. Los Sistemas Tecnológicos de Seguridad.
3. Los Procesos y sus Procedimientos.
4. Los Recursos Humanos.

III. DEFINICIONES

Data Center (DC): Es una infraestructura crítica. Donde se reciben, transmiten, procesan y almacenan datos e información perteneciente a Claro y sus clientes a nivel local, regional e internacional. Con determinadas características especiales de confiabilidad, protección y seguridad física, lógica, ambiental y de energía redundantes.

Para que bajo todas estas condiciones, asegurar la disponibilidad de los servicios con un gran valor estratégico para el desarrollo y continuidad del negocio de la compañía y sus clientes.


Infraestructura Crítica: Es aquella infraestructura o instalación generadora de servicios de necesidades esenciales, de carácter público o privado, que, en el caso de alguna interrupción total o parcial, ya sea por motivos indeseables antrópicos o naturales, impactaría a sus usuarios, clientes, a la sociedad, a la región, a un país o a varios países. Por tales motivos su consideración y protección es fundamental, tanto a nivel de seguridad lógica e informática como de seguridad física y electrónica.

Proceso: Es el grupo de actividades descritas a alto nivel, a partir de ciertas entradas para lograr una salida deseada. Están impulsados por la búsqueda de resultados y son dinámicos. Un proceso puede tener muchos procedimientos.

Procedimiento: Secuencia de pasos definidos en forma específica para ejecutar una tarea estructurada. Son estáticos y están pensados para tareas operativas.

SOC: Security Operations Center, Centro de Operaciones de Seguridad. Es el lugar en donde se concentran y convergen todos los sistemas de seguridad, realizándose la gestión de la seguridad física.

Sistema: Conjunto de cosas que relacionadas entre sí ordenadamente contribuyen a determinado objetivo.

	Política de Seguridad Física del Data Center	Código: POL 2011 Rev. 4	
		Fecha de vigencia: Según publicación	
	Responsables de la ejecución: Jefatura de Seguridad Física,	Aplicación: Claro Argentina	Pag:2 de 7

ISS: Integrity Security Systems, Sistema de Seguridad Integral.

MTTO: Servicio de Mantenimiento: Es el servicio contratado en que consiste un conjunto de actividades que tienen como propósito preservar y reactivar. Garantizándonos la conservación de una cosa en buen estado o en una situación determinada para evitar su degradación o pérdida, realizado por técnicos calificados y habilitados.

VSS: Video Surveillance System, Sistema de Video Vigilancia. Es un sistema de tecnología de vigilancia visual que implica la instalación de cámaras fijas o móviles, y equipos de almacenamiento, software de Gestión, en lugares estratégicos para que capten imágenes y las envíen a uno o varios puntos de visualización (locales o remotos).

IAS: Intrusión Alarm System, Sistema de Alarma de Intrusión. Es un elemento de seguridad pasiva. Esto significa que no evitan una situación anormal, pero sí son capaces de advertir de ella, cumpliendo así, una función disuasoria frente a posibles problemas. Pueden formar parte de este sistema, sensores de detección movimiento, sensores

PACS: Physical Access Control System, Sistema de Control de Acceso Físico.

Área: Es un grupo de sectores acotado, señalizado, protegido, dedicado, gestionado y específico, que se distingue de la que se rodea, mediante medios procesales y de políticas internas.

CL: Critical Levels, Niveles de Criticidad. En el Data Center definimos Áreas críticas con los siguientes Niveles de Criticidad: Alta, Media y Baja.

SL: Security levels, Niveles de Seguridad, Contamos con nivel de seguridad Alta, Media y Baja.


Sector: Parte de un área.

Salas Productivas: Son las salas más críticas del DC, existen los propios y de terceros.

Sector Recepción: Es el sector en donde un operador capacitado, atiende y recibe a los clientes, visitas, proveedores y colaboradores su función consiste en proporcionar todo tipo de información y asistencia, ajustándose a la confidencialidad y a nuestras políticas internas. Es aquí en donde informan a que lugares necesita acceder, a quien se viene a visitar o que material va a entregar.

Validación: Es el proceso de establecer evidencia documentada que proporciona un alto grado de seguridad de que un proceso de acceso específico, consistentemente produce un acceso que cumple las especificaciones y características de seguridad predeterminada.

Autorización: Es una parte del proceso de validación donde, mediante un acto documentado, una autoridad dentro de la jerarquía organizacional de CLARO, le permite o prohíbe el acceso, tarea y/o actividad a una persona dentro del DC y sus dependencias.

	Política de Seguridad Física del Data Center	Código: POL 2011 Rev. 4	
		Fecha de vigencia: Según publicación	
	Responsables de la ejecución: Jefatura de Seguridad Física,	Aplicación: Claro Argentina	Pag:3 de 7

Sector Control: Es el sector en donde se realiza la observación, inspección, verificación y registro de los elementos a acceder o a resguardar, por parte de un operador de seguridad física.

Sector Acreditación: Es el sector en donde el interesado a acceder, una vez ya validado, autorizado y controlado, procede a su registro en nuestro ACS, entregándole una credencial con su respectivo perfil y llave, según el tipo de personal.

ABM: Alta, Baja y Modificación de un perfil de acceso.

KMS: Key Management System, Sistema de Gestion de Llaves.

ACE: Access Control Equipement, es el proceso en que todos nos tenemos que regir, para el acceso de equipamiento de la organización o del cliente. Este acceso cuenta con un procedimiento de información, verificación, autorización, registro y archivo, en donde se confecciona el formulario oficial validado por CLARO.

FPS: Fire Prevention System, Sistema Contra el Incendio.

ES: Evacuation System, Sistema de Evacuación, son los dispositivos que actúan ante un siniestro y así garantizar la evacuación efectiva de toda la infraestructura. Estos dispositivos forman parte del Plan de Evacuación.

Plan de Evacuación: Es la planificación y organización humana para la utilización óptima de los medios técnicos y organizativos previstos con la finalidad de reducir al mínimo las posibles consecuencias que pudieran derivarse de una situación de riesgo.


El plan de evacuación es una forma de actuación que se debe elaborar para que cada persona involucrada sepa lo que tiene que hacer y llevarlo a la práctica en el menor tiempo posible.

BCMS: Business Continuity Management System, Sistema de Gestión de la Continuidad del Negocio. Especifica los requisitos para planificar, establecer, implementar, operar, monitorear, revisar, mantener y mejorar continuamente un sistema de gestión documentado, para proteger reducir la probabilidad de ocurrencia, prepararse, responder y recuperarse de incidentes perturbadores.

Plan de Contingencia: Un Plan de Contingencias es un instrumento de gestión para el manejo de las Tecnologías de la Información y las Comunicaciones en el dominio del soporte y el desempeño. Dicho plan contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del negocio y las operaciones de nuestra compañía.

Operador: Es un recurso humano capacitado, a quien se le asigna un usuario validado y autorizado para utilizar un sistema, para el propósito para el cual está destinado.

Recorrida: Es un complemento de acción a nivel preventivo, consistente en recorrer todo el DC, observando y corroborando la efectividad de la protección y el normal funcionamiento de los dispositivos que hacen la seguridad física y electrónica, y colaborativa a nivel de Infraestructura y Operaciones del DC. Esta acción es realizado por el servicio de vigilancia un operador de Seguridad Física.

	Política de Seguridad Física del Data Center		Código: POL 2011 Rev. 4	
			Fecha de vigencia: Según publicación	
	Responsables de la ejecución: Jefatura de Seguridad Física,		Aplicación: Claro Argentina	Pag:4 de 7

Gestión: es la realización de un conjunto de acciones para poder lograr los objetivos y las metas de la organización.

HPSM: HP Service Manager es la solución de Gestión de Servicios integrada y modular que permite a la Organización mejorar sus niveles de servicio. Permite de forma rápida y eficiente implementar procesos consistentes e integrados para cada área de la organización.

Requerimiento: Se puede definir como un atributo necesario dentro de un sistema, que puede representar una capacidad, una característica o un factor de calidad del sistema de tal manera que le sea útil a los clientes o a los usuarios finales. Un requerimiento es una descripción de una condición o capacidad que debe cumplir un sistema, ya sea derivada de una necesidad de usuario identificada, o bien, estipulada en un contrato, estándar, especificación u otro documento formalmente impuesto al inicio de un proceso.

Incidente: Cualquier evento que no forma parte del desarrollo habitual del servicio y que causa, o puede causar una interrupción del mismo o una reducción de la calidad de dicho servicio. El objetivo es reiniciar el funcionamiento normal tan rápido como sea posible con el menor impacto para el negocio y el usuario con el menor coste posible.

SLA: Service Level Agreement (SLA) es un nivel de acuerdos que describe el nivel de servicio que un cliente espera de su proveedor.

ISS: Sistema de Seguridad Integral: es el conjunto de sistemas tecnológicos, humanos, físicos organizativos, procesales y estructurales, dedicados a brindar y a garantizar la seguridad, protección y confiabilidad en las operaciones de la organización.

IV. LINEAMIENTOS

A. GENERALES

La Jefatura de Seguridad Física es el área que facilitará, gestionará y garantizará un **Sistema Seguridad Integral (ISS)** para el Data Center Olleros. Con el fin de mitigar riesgos potenciales y resguardar los bienes tangibles e intangibles, para obtener como resultado la confiabilidad y la protección del negocio y operaciones de CLARO y nuestros clientes.


El **Sistema de Seguridad Integral (ISS)** brindará un nivel de Seguridad acorde a la Criticidad de cada Área de Infraestructura y Operativas que abarcan el Data Center.

La ISS será distribuida bajo el concepto de capas de seguridad, desde las áreas periféricas externa del DC hacia las partes internas y según nivel de criticidad para la operatoria.

La Criticidad de Áreas y Nivel de Seguridad se establecen en el Anexo I de la presente política.

El Sistema de Seguridad Integral (**ISS**) está compuesto por los principales sistemas tecnológicos:

- 1) **Sistemas de Seguridad Electrónica:**
- 2) **Sistemas de Seguridad Física:**

	Política de Seguridad Física del Data Center	Código: POL 2011 Rev. 4	
		Fecha de vigencia: Según publicación	
	Responsables de la ejecución: Jefatura de Seguridad Física,	Aplicación: Claro Argentina	Pag:5 de 7

En el DC, contará con un servicio de mantenimiento preventivo y correctivo dedicado en los sistemas de IAS, ACS y VSS respectivamente, con acuda de emergencia.

En caso de alguna interrupción del normal funcionamiento de alguno de los sistemas o de sus dispositivos, se realizará un incidente en HPSM, ya sea por parte de los operadores de seguridad física o colaboradores de otro sector.

B. PARTICULARES

Las particulares del Sistema de Seguridad Integral (ISS) se describen a continuación:

1) *Sistemas de Seguridad Electrónica:*

Es el conjunto de sistemas que conforman y brindan la seguridad y protección de los activos y bienes, propios y de terceros. Estará conformado por:

VSS: Sistema de Video Vigilancia:

Es un sistema de vigilancia visual que combina cámaras de video vigilancia, dispositivo de almacenaje de imágenes, software de Gestión.

Sus ubicaciones, distribución y cantidad son estratégicas, será la estipulada por la criticidad de cada área y nivel de seguridad exigido para la misma.

Este sistema será operado localmente las 24 horas del día por un operador del SOC. Con fines preventivos y de evidenciar incidentes. Contando con una redundancia de monitoreo en el puesto de seguridad ubicado estratégicamente sobre el acceso secundario del DC (Calle Amenabar).

Se cuenta con el software de gestión Victor, que está integrado al ACS.


El almacenaje del sistema cuenta con 04 NVR (Network Video Record) activos y 02 backup. Estos NVR pasivos, se activan por si se dañase uno o mas NVR, a modo de contingencia. (Será de N+2 NVR)

Todo el sistema está conectado a energía securizada, garantizando así su disponibilidad y funcionamiento. Si surgiera alguna interrupción del servicio del sistema, será catalogado como un incidente por medio del HPSM.

En cuanto a la disponibilidad del sistema contará con un almacenaje que garantice los 90 días de registros.

IAS: Sistema de Alarma de Intrusión:

Es un elemento tecnológico de seguridad pasiva. Esto significa que no evitan una situación anormal o un intento de acceso no validado o autorizado, pero sí son capaces de advertir de ella, cumpliendo así, una función disuasoria frente a posibles problemas. Una vez que la alarma comienza a funcionar, contamos con un procedimiento de acción, por parte del operador abocado a este rol las 24 horas del día y los 7 días al año. En el DC, este sistema está integrado en nuestro ACS y VSS.

	Política de Seguridad Física del Data Center	Código: POL 2011 Rev. 4	
		Fecha de vigencia: Según publicación	
	Responsables de la ejecución: Jefatura de Seguridad Física,	Aplicación: Claro Argentina	Pag:6 de 7

PACS: Sistema de Control de Acceso Físico.

Este sistema tecnológico de seguridad, está integrado con las barreras físicas (puertas o rejas) y estructurales (paredes y alambrados), el IAS, VSS y de procesos de acceso respectivamente.

Toda ABM, será gestionado por vía de HPSM.

Este sistema también está conformado por los dispositivos electrónicos, como cerraduras electromagnéticas, lectores de tarjetas, PIN y biométricos, sirenas y dispositivos de emergencia, como también un software de gestión y de supervisión, que es operado las 24 horas y los 7 días al año. Haciendo así los círculos concéntricos o capas de seguridad y protección, según el perfil y el SL requerido.

KMS: Sistema de Gestion de Llaves.

Este sistema tecnológico electrónico/mecánico es desarrollado para proteger, resguardar, almacenar, controlar, supervisar y registrar la distribución de retirada y devolución de llaves, por medio del HPSM. El cofre contenedor blindado ignífugo de resguardo de llaves está protegido con un sistema de clave para poder acceder al panel de las llaves, con acceso solo de un operador de seguridad física validado y autorizado.

Toda entrega de llave tiene que estar justificada y autorizada, ya que es el sistema más crítico, ya que con estas llaves se acceden a sectores críticos y al epicentro de nuestros círculos concéntricos o a la última capa de protección y seguridad que son los racks.

2) Sistema de Seguridad Humana:

Equipo de operadores de seguridad física:

Es el equipo humano capacitado, habilitado, validado, y autorizado, para cumplir y hacer cumplir las políticas y normativas impuestas en la organización en cuanto a seguridad física se refiere. Es el personal que a su vez es fundamental y necesario para interactuar y complementar el ISS.

Recorrida:

El objetivo de la recorrida en todo el DC es el de prevenir, detectar, identificar, informar posibles riesgos o incidentes, en toda la instalación, que impactaran en la normal operatividad y funcionamiento del DC, como también así de verificar el estado y funcionamiento de todas las puertas incluyendo los racks y su interior, para poder así generar un incidente a las áreas correspondientes para su resolución.

Mtto: Servicio de Mantenimiento:


El objetivo del Mtto, es asegurar la disponibilidad y confiabilidad prevista de las operaciones con respecto de la función deseada, dando cumplimiento además a todos los requisitos del sistema, de los procesos y de los SLA internos y externos.

Contamos con el mtto integrado de conservación, preventivo, correctivo, emergencia y de oportunidad de actualización y mejora.

En el DC contamos con un Mtto exclusivo y dedicado al ISS, realizado por una empresa de primer nivel, que cuenta con personal habilitado para la tarea.

Este servicio es supervisado y certificado por personal de seguridad física.

Situaciones de Riesgo:

	Política de Seguridad Física del Data Center		Código: POL 2011 Rev. 4
			Fecha de vigencia: Según publicación
	Responsables de la ejecución: Jefatura de Seguridad Física,	Aplicación: Claro Argentina	Pag:7 de 7

Las situaciones de riesgo, son las probabilidades de que se produzcan un daño o interrupción de la operatividad del DC, causado por diversos factores o situaciones. Estos riesgos deben de ser identificados, analizados y tratados específicamente en cada sector o área concreta.

V. RESPONSABILIDADES

Jefatura de Seguridad Física: Velar por el cumplimiento de esta política y el mantenimiento de los sistemas de seguridad electrónica instalados en Data Center.

Jefes y Gerentes de Data Center Olleros: Velar por el cumplimiento de esta política y el correcto uso de los sistemas de seguridad electrónica instalados en el edificio.

Analistas/Supervisores/Administradores: Efectuar el correcto uso de los sistemas de seguridad electrónica instalados.

VI. ANEXOS

Anexo I - Matriz de Requisitos de Áreas Según su Criticidad.

VII. SUSTENTO NORMATIVO TÉCNICO Y LEGAL

Ley 25326

Ley 2602

IRAM 62676-1: 2016. Sistemas de Video Vigilancia (VSS) para uso de aplicaciones de Seguridad. Parte 1 Requisitos de los Sistemas.

Ley 2854

IRAM 4175: 2008. Sistemas de alarma de intrusión en inmuebles. Código de práctica para la planificación y la instalación.

IRAM- 4176: 2014. Sistemas de alarma contra la intrusión y el asalto en inmuebles. Requisitos generales de desempeño considerando grados de seguridad y clases ambientales.

IRAM- 4177: 2012. Sistemas de alarma. Instalación y configuración de sistemas de alarma diseñados para generar condiciones de confirmación de alarma. Código de práctica.

UNE-EN 50133-7:2000. Sistemas de alarma. Sistemas de control de accesos de uso en las aplicaciones de seguridad. Parte 7: Guía de aplicación.

UNE-EN 60839-11-1:2014. Sistemas electrónicos de alarma y de seguridad. Parte 11-1: Sistemas electrónicos de control de acceso. Requisitos del sistema y de los componentes.

UNE-EN 60839-11-2:2015. Sistemas electrónicos de alarma y de seguridad. Parte 11-2: Sistemas electrónicos de control de acceso. Guía de aplicación.