



UNIÓN TEMPORAL RECLAMACIONES 2023

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN – CPS-1004-2023

CONTENIDO

Marco Conceptual

1. Política de Seguridad Física y del Entorno
2. Seguridad Física y del Entorno
3. Política de Seguridad de la Información
4. Política de Ciberseguridad
5. Protección frente a virus y software malicioso
6. Política de Backup
7. Respaldo de Información
8. Gestión de Incidentes
9. Política de Tratamiento de Datos Personales
10. Capacitaciones Seguridad de la Información



MARCO CONCEPTUAL

De conformidad con las estipulaciones del Contrato de Prestación de Servicios 1004 de 2023 suscrito con ADRES, en especial lo contenido en el Anexo No. 3 Especificaciones Técnicas Generales, numeral 4. Requerimientos Tecnológicos, subnumeral 4.3 Sistema de Seguridad y Control del Sistema de Información, la Unión Temporal Reclamaciones 2023 adoptó las políticas de seguridad de la información para los lotes 3 y 4, las cuales se presentan a continuación.

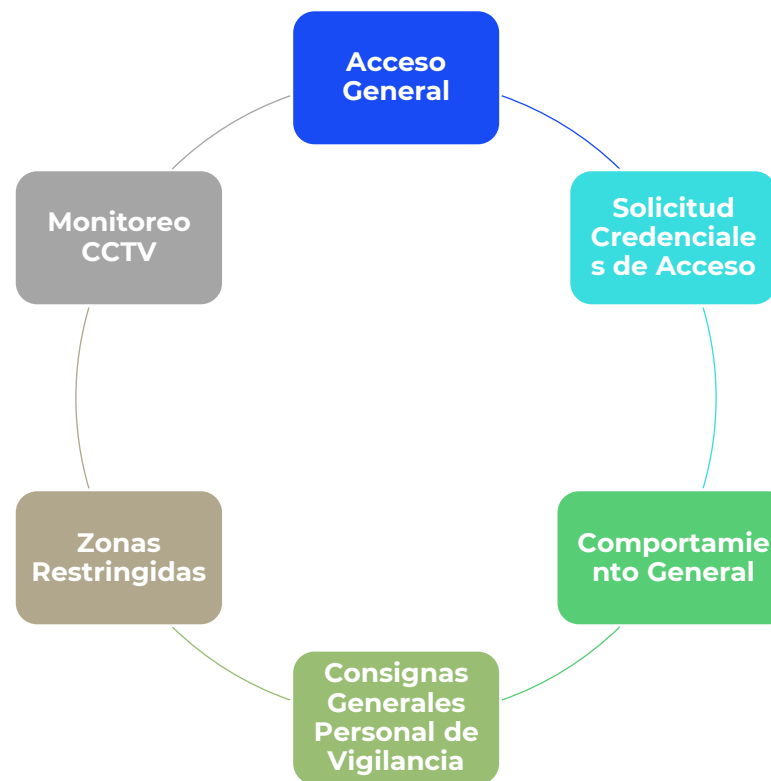
ADRES

POLÍTICA DE SEGURIDAD FÍSICA Y DEL ENTORNO (S-SI-03)

Establecer directrices generales referentes a Seguridad Física que aseguren el acceso general a las diferentes sedes, zonas restringidas, solicitud de credenciales de acceso, consignas generales del personal de vigilancia, monitoreo CCTV y comportamiento general para toda la organización y clientes.



CIRCUITO
CERRADO DE
TELEVISIÓN
GRUPO ASD



2 | SEGURIDAD FÍSICA Y DEL ENTORNO

SEGURIDAD DE OFICINAS, DESPACHOS Y RECURSOS

- Equipos de cómputo asegurados en puestos de trabajo.
- Ubicación de equipos y medio de respaldo en áreas seguras.
- No información sensible en puestos de trabajo
- Regulaciones del Sistema de Gestión de Seguridad y Salud en el Trabajo.

PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y AMBIENTALES

- Equipos contraincendios.
- Identificación de riesgos relacionados con desastres naturales terremotos, inundaciones, explosión, etc.
- Ubicación de equipos y medio de respaldo en áreas seguras.

SEGURIDAD PERIMETRAL

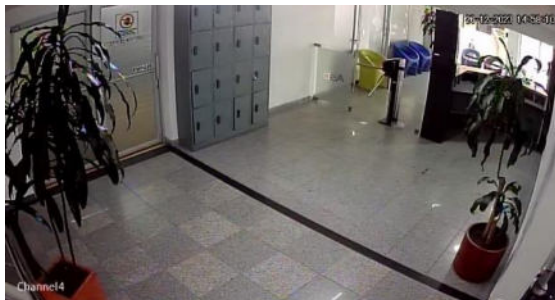
- Análisis de Riesgos del Entorno.
- Revisión eventos inusuales en la periferia de las instalaciones.
- Vigilancia 7x24.
- Sistema CCTV.
- Barreras perimetrales.
- Comunicación con el cuadrante de la Policía

BARRERAS DE CONTROL DE ACCESO FÍSICO

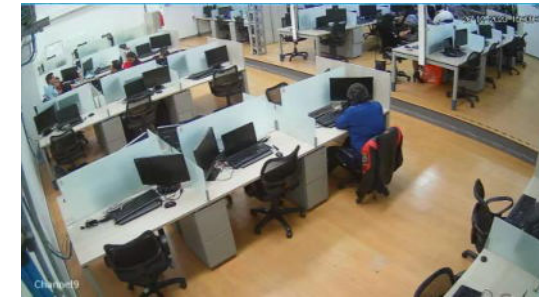
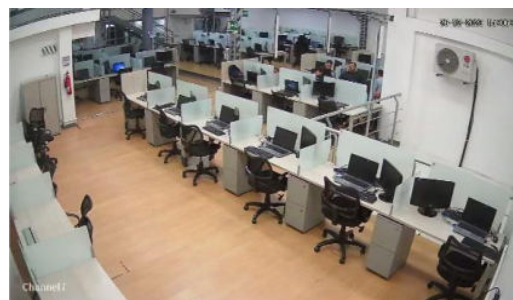
- Control de acceso biométrico en 1 anillo de seguridad.
- Control de acceso de funcionarios, visitantes y terceros.
- Guardas de vigilancia 7x24 en todas las sedes.
- Monitoreo CCTV.
- Definición de zonas seguras para evitar daños e interferencias.

2 | SEGURIDAD FÍSICA Y DEL ENTORNO

Entradas y Salidas



Piso 2 Adres



Piso 1 Adres



Zonas Comunes



Identificar y salvaguardar los activos de información, protegiendo la disponibilidad, integridad y confidencialidad de la información de clientes y empleados, comprometiéndose a desarrollar, implantar, mantener y mejorar continuamente el sistema de gestión de seguridad de la información.



INDICADORES DE GESTION

- Efectividad a respuesta de incidentes
- Efectividad a respuesta de eventos
- efectividad en mitigación de hallazgos
- Riesgos Mitigados

4 | POLÍTICA DE CIBERSEGURIDAD (S-SI-02)

Establecer lineamientos para prever y mitigar el riesgo tecnológico en que se pueda incurrir, con el fin de asegurar el correcto funcionamiento de la infraestructura tecnológica y la continuidad de las operaciones.



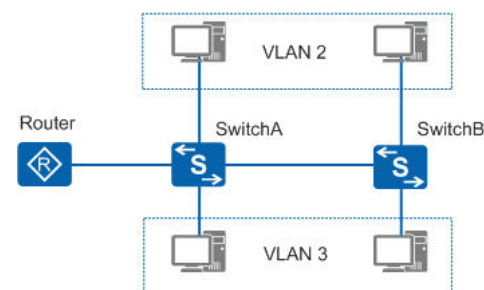
KASPERSKY



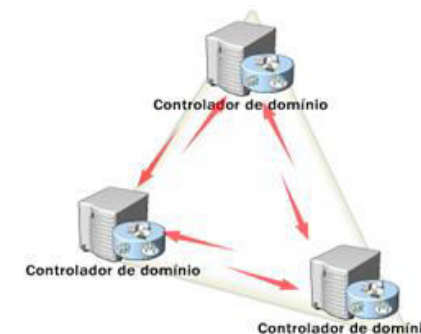
FIREWALL



VLAN



DOMINIO



RESPALDO DE LA INFORMACIÓN



PROHIBICIÓN EN INSTALACIÓN DE SOFTWARE



6 | POLÍTICA DE BACK UP

Política de Backup

Código de la Política

S-SI-02 POLÍTICA DE CIBERSEGURIDAD.

COPIAS DE SEGURIDAD:

Establecer medios de respaldo adecuados para asegurar la continuidad de la operación:

- La política general de copias de seguridad (Backup) es transversal a todos los procesos.
- Asegurar la continuidad de la operación, todo esto al establecer un plan de respaldo y recuperación de información sensible.

7 | RESPALDO DE LA INFORMACIÓN

Servicio	Servidor Principal	Horario de backup	Servidor Respaldo
Aplicación LYRA	10.0.5.66	Todos los días a las 22:00 horas	10.0.4.147
Aplicacion ORION	10.0.4.56	Todos los días a las 01:00 horas	10.0.4.147
Base de Datos Orion	10.0.4.43	Todos los días a las 01:00 horas	10.0.4.147
Base de Datos lyra_orion	172.16.0.25	Todos los días a las 05:00 horas y 17:00 hora	172.16.0.7
Carpeta Compartida	10.0.5.115	Todos los días a las 22:30 horas	10.0.4.147

Política de Retención de los Backups

- 1 Únicamente se mantendrán almacenados los backups mensuales organizados por año.
- 2 Se mantendrán almacenados los backups semanales durante el transcurso del mes, al final del mismo estos serán eliminados y se mantendrá únicamente el mensual.
- 3 Se mantendrán almacenados los backups diarios durante el transcurso de la semana, al final de la misma estos serán eliminados y se mantendrá únicamente el semanal.

NOTA: Finalizado el año respectivo, únicamente se mantendrá el ultimo backup mensual que se haya generado.

8 | GESTIÓN DE EVENTOS E INCIDENTES

Gestión de Eventos e incidentes SI

Código del procedimiento

P-SI-01 PROCEDIMIENTO DE GESTIÓN DE EVENTOS E INCIDENTES DE SEGURIDAD DE LA INFORMACION.



POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES (S-SI-04)



Principios y garantías de protección en ejercicio de derecho constitucional



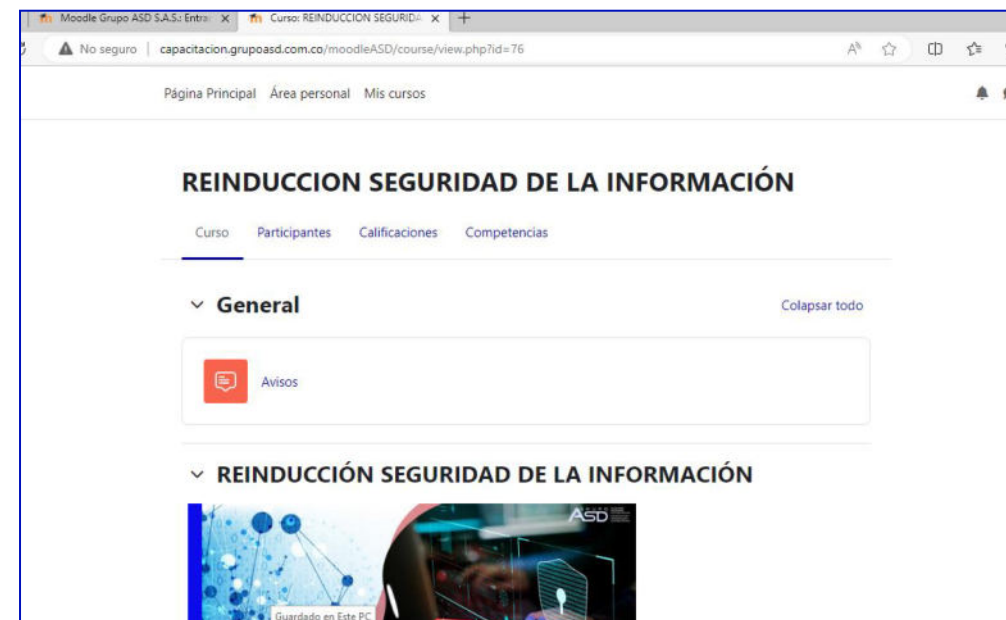
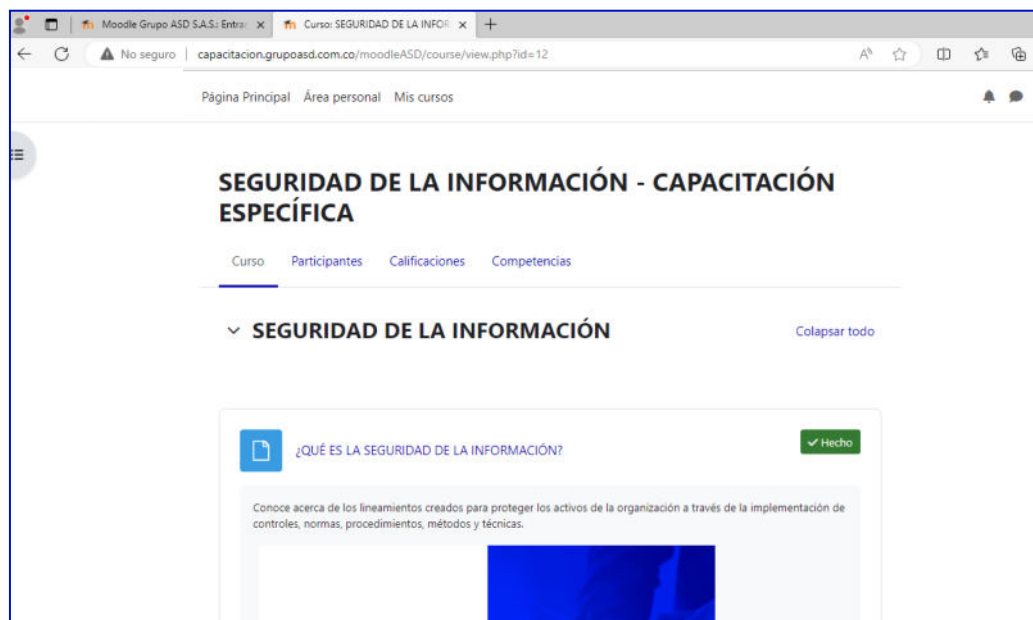
Ley 1581 de 2012, Decreto Reglamentario 1377 de 2013, Decreto 886 de 2014



Actualizar, rectificar y suprimir información personal

[Política de tratamiento de datos personales](http://www.grupoasd.com)
www.grupoasd.com





tecnología+
innovación
=futuro

Carrera 8 # 46 - 35
Tel: (1) 3402501
Bogotá – Colombia
grupoasd.com.co