Experiencia del Aeropuerto Internacional El Dorado en la Implementación del SeMS

EL DORADO
Nuevo mundo. Nuevas conexiones.

¿Quiénes somos?

El concesionario Opain, de mayoría accionaria de Odinsa, **es el encargado de administrar, modernizar, expandir, operar, mantener y comercializar el Aeropuerto**, que es hoy por hoy, es una de las obras de infraestructura más importantes de Colombia.

Nuestro actuar está enmarcado dentro del cumplimiento del contrato concesión, calidad de los servicios, los principios de responsabilidad social, protección del ambiente, bienestar, seguridad y salud de sus usuarios y empleados.


El Dorado,
MEJOR AEROPUERTO
de Sudamérica según Skytrax
WORLD TRAVEL AWARDS
WINNER
WORLD AIRPORT
WINNER
SKYTRAX
AWARDS 2022
Además,
¡SOMOS EL AEROPUERTO
LIDER DE AMÉRICA DEL SUR,
según los World Travel Awards!

El Dorado recibe reconocimiento en los premios Airports Going Green Award.

La revista International AirPort Review, destaca la modernización de la señalización en El Dorado.

El Dorado ganó en los XVI Premios Lazos en la categoría Acción por el Clima.

El Dorado obtiene certificado de la ACI sobre mejora de Accesibilidad.

Llega a El Dorado nuestra asistente virtual, DoraBot.

DoraBot, es una herramienta de inteligencia artificial que ofrece una atención personalizada y amable.

Esta asistente fue diseñada para resolver las dudas de los viajeros y brindar información al instante sobre viajes, estado de los vuelos, tiempos de fila, servicios, locales comerciales, y mucho más.

AIRPORTS COUNCIL INTERNATIONAL

- La Paz
- Los Cabos
- Puerto Vallarta
- Hermosillo
- Morelia
- Aguascalientes
- Tijuana
- Sinaloa

SeMS

1

Compromiso de la Dirección

- *Apoyo por parte de la alta Gerencia*
- *Política y Objetivos*
- *Responsabilidades de Seguridad Aeroportuaria*
- *Revisiones Gerenciales*

2

Recursos

- *Provisión de Recursos*
- *Designación de Personal Clave*
- *Especificación de Equipos*
- *Supervisión Eficaz a Terceros*

3

Gestión de Amenazas y Riesgos

- *Proceso para manejar amenazas Locales*
- *Proceso para Evaluar y calificar las Amenazas*
- *Proceso para Evaluar los Riesgos*
- *Identificación y Seguimiento*

4

Vigilancia y Mejora Continua

- *Medición de la Eficacia*
- *Análisis de Datos*
- *Reportes de Eficacia*
- *Almacenamiento de Documentos*

5

Respuesta Ante Incidentes

- *Método para mejorar el proceso de respuesta*
- *Programa de Instrucción SeMS Capacitación Interna y Externa*

6

Generales

- *Actas*
- *Funciones de Apoyo Administrativo*

7

Comunicación

- *Medidas para comunicar eficazmente, Boletines, Security Awarenes*

EL DORADO

Nuevo mundo. Nuevas conexiones.

Experiencia del Aeropuerto El Dorado con respecto a la Implementación

Nuevo mundo. Nuevas conexiones.

OBJETIVO

Gestionar apropiada y sistemáticamente los riesgos de seguridad aeroportuaria, en el aeropuerto Internacional El Dorado Luis Carlos Galán Sarmiento, a partir del desarrollo y cumplimiento de procedimientos por parte de la **comunidad aeroportuaria y OPAIN S.A**., buscando mantener una operación segura dando cumplimiento a la normatividad vigente aplicable.

Componentes Retadores

01. Identificación de Fuentes de Riesgo Externas y Seguimiento

02. Que Tenedores de Espacio, Contratistas y Proveedores conozcan el plan de seguridad del aeropuerto, mantengan su plan de seguridad aprobado, actualizado y que este sea radicado ante Opain.

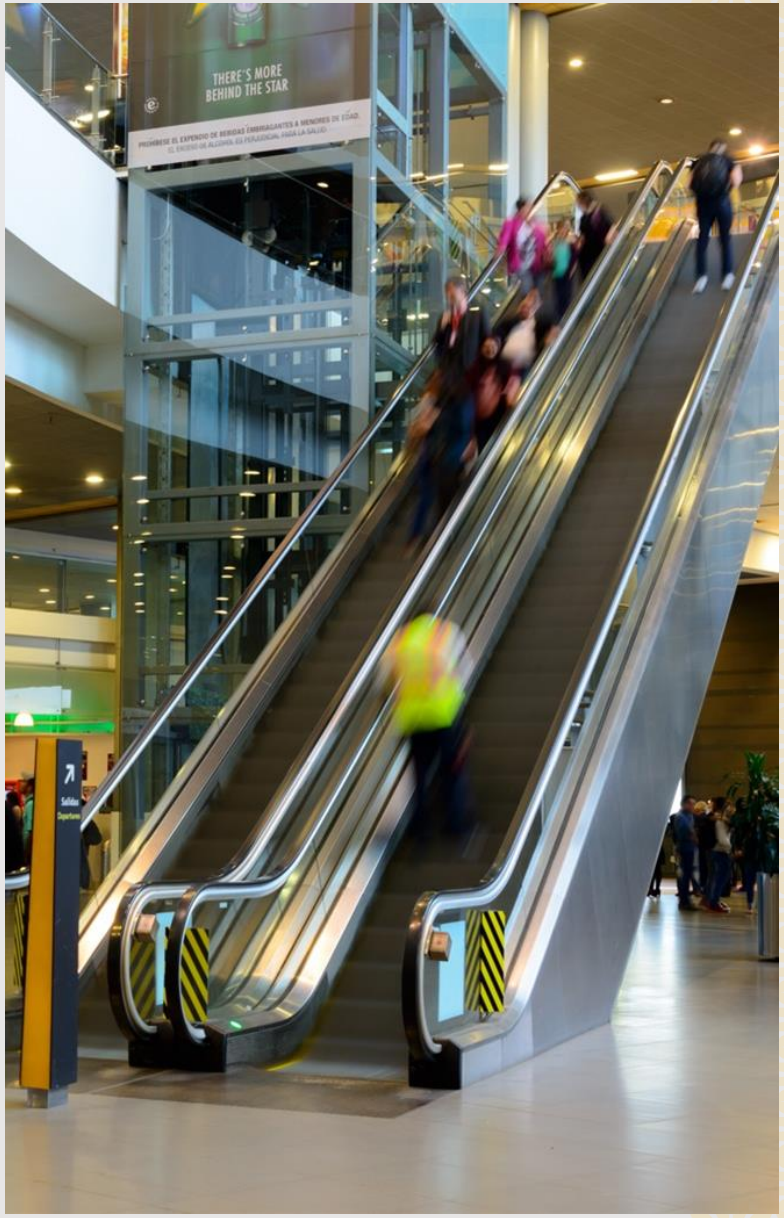
03. Obligados realicen los planes de acción y las mejoras correspondientes en temas de seguridad aeroportuaria de acuerdo a las inspecciones realizadas.

Componentes Retadores

04. Temáticas de Simulacros-Plan de Mejora

05. Alta Rotación-Entrenamientos, curvas de aprendizaje

06. Alta Dirección se asegure que la política de Seguridad del SeMS sea comunicada y entendida por toda la organización



Componentes Retadores

07. Mantener Instrucción sobre el SeMS para todo el personal afectado por la implementación del SeMS y que tiene responsabilidad sobre cada uno de los componentes

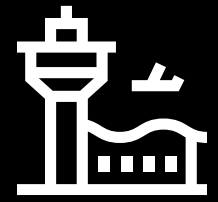
08. Ciber seguridad- Anexo 26 PSA

PLAN DE RESPUESTA A INCIDENTES DE SEGURIDAD DIGITAL PARA LA INFRAESTRUCTURA TECNOLÓGICA AEROPORTUARIA

Adjunto 25 al RAC 160 – Seguridad de la Aviación Civil, CIBER AMENAZAS

Decreto 338 del 8 de marzo de 2022 por el cual se establecen los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones, del Ministerio de la Tecnología de la Información y las Comunicaciones

Documento Directrices de respuesta a incidentes de ciberseguridad del Consejo Internacional de Aeropuertos – ACI (ACI, 2022)



Marco de ciberseguridad para la protección de infraestructuras críticas (Cibersecurity Framwork Core – CSF), del Instituto Nacional de Estándares y Tecnologías (NIST, por su sigla en inglés).

PASOS PRUEBA DE ESCRITORIO

Objetivo: Desarrollar un ataque de intermitencia en el servicio al sistema AMS.

Participantes: OPAIN (Tecnología, Operaciones, Riesgos, Seguridad Aeroportuaria), SOFISTIC, SITA, COLLINS y JHONSON.

Tipo de ataque: Ransomware: *"…bloquea los archivos del usuario y exige un rescate para desbloquearlos. "*

Vector de ataque: Un administrador del CGSA transgrede archivos de configuración del servidor en la plataforma donde se aloja los sistemas

Blanco: Afectar la asignación de recursos en el Aeropuerto y cobrar un rescate para recuperar la normalidad de la operación.

Contexto: El CCO evidencia intermitencia en el sistema al realizar el cargue y actualización de los recursos de la terminal.

Mensajes: Desarrollar por cada área los mensajes previos a la situación. Se activará el Comité de Crisis – Plan de Seguridad?

Día y horario: 30-Nov-23 y cerrar horario con responsables y actividades definidas en el Plan de Continuidad.

Preoperativos: Diligenciamiento de formatos de simulacros de OPAIN teniendo en cuenta la información socializada 3 días antes de la fecha definida.

ACTIVACIÓN PLAN DE RESPUESTAS A INCIDENTES DE SEGURIDAD DIGITAL PARA LA INFRAESTRUCTURA TECNOLÓGICA

Objetivo

Políticas y procedimientos ante incidentes, amenazas o actos de interferencia ilícita, con alcance seguridad digital o ciberseguridad.

Marco políticas y mejores prácticas

- Decreto 338/2022. Gobernanza Seguridad Digital;
- Adjunto 25 RAC 160 de la Aerocivil;
- Directrices de respuesta a incidentes de ciberseguridad del Consejo Internacional de Aeropuertos –ACI;
- Marco de ciberseguridad para la protección de infraestructuras críticas del Cibersecurity Framework Core CSF y marco de gestión de la Seguridad Digital – NIST;
- Contrato de concesión: Apéndice E – Sistemas Especiales.

Equipo Sistemas Aeroportuarios

- Director Tecnología Aeroportuaria y Corporativa;
- Jefe Continuidad Tecnológica;
- Coordinación Continuidad Tecnológica;
- Coordinación Infraestructura Corporativa;
- Ingeniero de Infraestructura;
- Aliado Estratégicos:
  - Sistemas Aeroportuarios
  - Equipo Gestión de Incidentes
  - Equipo Gestión de Recuperación

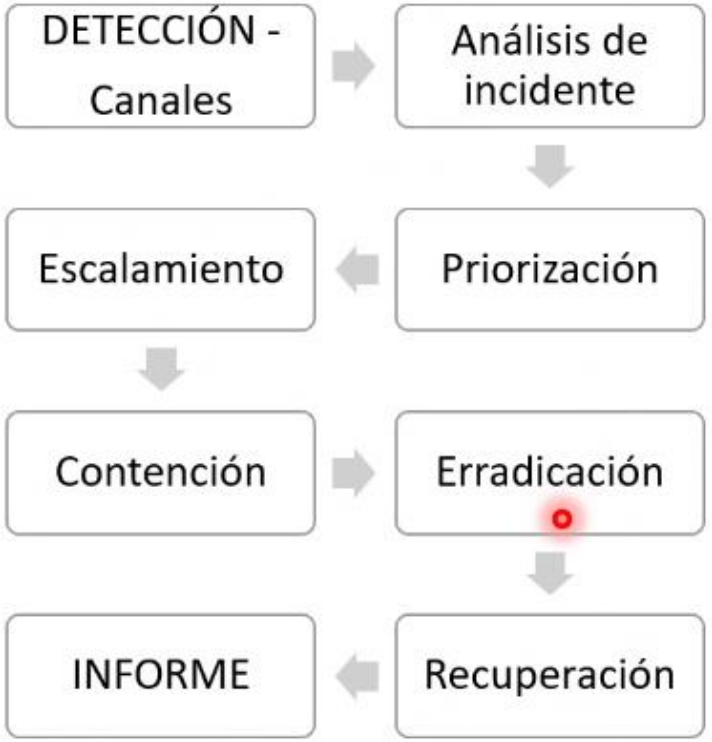
Equipo Seguridad Digital

Director Telecomunicaciones & Seguridad Digital
Coordinador Telecomunicaciones;
Ingeniero de Seguridad Digital;
Ingeniero Telecomunicaciones;
Aliado Estratégicos:

- Equipo Gestión de incidente: Sofistic;
- Equipo Gestión recuperación del servicio: Liberty Networks;
- Procesos: NDV.

ACTIVACIÓN PLAN DE RESPUESTAS A INCIDENTES DE SEGURIDAD DIGITAL PARA LA INFRAESTRUCTURA TECNOLÓGICA

Fases de la gestión de incidentes



Calificación del ataque

Categorías de urgencia de un incidente		
Nivel para calificar la urgencia (U)	Porcentaje de activos de información y tecnología de los Sistemas Aeroportuarios involucrados (cuantitativo)	Tiempo de afectación de activos de información y tecnología de los Sistemas Aeroportuarios
Muy Alto	Porcentaje de Sistemas Aeroportuarios afectados >50%	Tiempo por interrupción operaciones aeroportuarias >= 24 horas
Alto	Porcentaje de Sistemas Aeroportuarios afectados <50%	Tiempo por interrupción operaciones aeroportuarias >= 12 horas
Medio	Porcentaje de Sistemas Aeroportuarios afectados <10%	Tiempo por interrupción operaciones aeroportuarias >= 6 horas
Bajo	Porcentaje de Sistemas Aeroportuarios afectados <1%	No hay interrupción de las operaciones de Sistemas Aeroportuarios en El Dorado

Tiempos de gestión de incidentes de seguridad digital				
Prioridad	Detección	Identificación	Notificación	Solución
P1	10 minutos	10 minutos	10 minutos	2 horas
P2			20 minutos	6 horas
P3			30 minutos	12 horas

EL DORADO
Nuevo mundo. Nuevas conexiones.

COMITÉ DE CONTINUIDAD

GESTIÓN GLOBAL Y POR ESCENARIOS

Comité de Continuidad

PRINCIPAL	SUPLENTE 1	SUPLENTE 2
Gerente General	**Gerente de Operaciones**	**Gerente de Infraestructura**
Gerente de Operaciones	Director(a) de Operaciones	Director(a) de Seguridad Aeroportuaria
Gerente de Infraestructura	Director(a) de Mantenimiento Electromecánico	Director(a) de Mantenimiento Civil
Gerente Financiero y de Compras	Director(a) de Compras	Director(a) de Contabilidad y Data
Gerente de Gestión Humana y Tecnología	Director(a) Administrativo	Director(a) de Talento y Cultura Organizacional
	Director(a) de Tecnología Aeroportuaria y Corporativa	Director(a) de Telecomunicaciones y Seguridad Digital
Gerente de Asuntos Legales	Director(a) Legal Contractual	Director(a) Legal de Asuntos Legales y Corporativos
Gerente Comercial	Director(a) Inmobiliaria	Director(a) de Experiencia y Servicio

Ger. Infraestructura:
- Falla o Incendios en equipos críticos: Subestaciones eléctricas.

Ger. Gestión Humana y Tecnología:
- Ciberataques y otros incidentes tecnológicos.

Ger. operaciones o Ger. Infraestructura:
- Terremoto.
- Incendios en Instalaciones.
- Inundaciones por el río Bogotá.

PROCESOS Y SERVICIOS CRÍTICOS (TECNOLÓGICOS)

Procesos		Servicios críticos	Actividades
	Gestión de Operaciones	Terminal de pasajeros	*Check-In *Sistema de equipajes *Filtros de Seguridad Permisos (Migración, ICA, DIAN, Policía) *Comunicación en pantallas Ascensores y escaleras *Sistemas de información *Sistemas de comunicaciones
	Gestión ARFF Gestión de Mantenimiento Gestión de Seguridad Operacional Gestión de Operaciones	Plataforma	*Puentes de abordaje *Sistema de comunicaciones *Sistema de equipajes Drenajes o canales de agua lluvia Mantenimiento de equipos (Camión Barredora, etc). Control de Fauna y flora FOD Operaciones de salvamento y extinción de incendios *Instalaciones de emergencia (salvamento y extinción de incendios) *Asignación recursos operativos lado aire
	Gestión de Tecnología	Servicios y recursos tecnológicos	Computadores Administración de servidores virtuales Almacenamiento de los servidores virtuales Backup de todos los servidores virtuales y físicos Aplicaciones oficina ERP Facturación Carnetización

EL DORADO
Nuevo mundo. Nuevas conexiones.

FASES DE LA GESTIÓN DE CONTINUIDAD

Actuación Inicial

- **Recepción:** (fallo/Evento).
- **Análisis.**
- **Evaluación** (verificación).
- **Notificación inicial.**

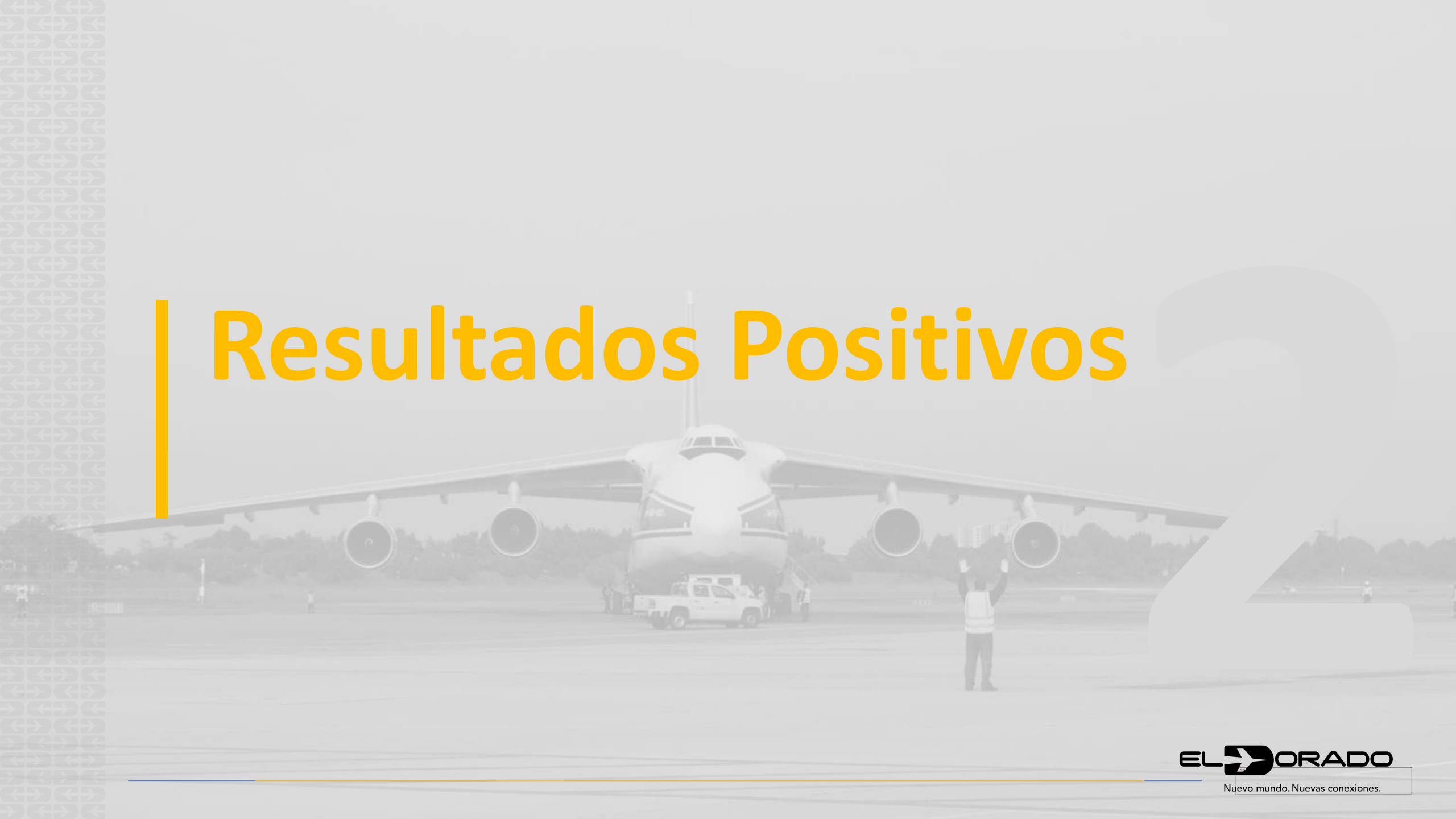
Actuación en curso

- **Activación:** (Plan de Continuidad del Negocio y de la Tecnología).
- **Gestión:** (fallo/Evento).
- **Contención, erradicación y recuperación.**

Actuación final

- **Cierre:** (fallo/Evento).
- **Notificación final.**

Resultados Positivos



Nuevo mundo. Nuevas conexiones.

- Apalancamiento con la Tecnología : Cámaras (video analítica), Veripax, equipos BHS, implementación del tomógrafo para equipajes en los filtros, equipo 920CT escaner de ondas milimétricas (adheridos), OSSTO reconocimiento facial, evaluación de propuestas para la detección de explosivos, sistema Xovis,(flujo de pasajeros en procesos Veripax y filtros de seguridad para detección de alertas tempranas), BIOMIG, Puertas Anti retorno, etc

- Buenas Relaciones con las Autoridades, apoyo oportuno en situaciones de seguridad.

- Sharepoint- Robusta Biblioteca de Datos que alimenta el sistema de reporte para dar enfoque en la gestión de riesgos

- Isolucion-Plan de mejora Continua para pruebas de seguridad y oportunidades de mejora evidenciadas de los simulacros