Ciberseguridade

A dixitalización multiplica os puntos de contacto co viaxeiro e, con eles, a exposición a incidentes de seguridade. Ciberseguridade e protección de datos son palancas estratéxicas que salvagardan continuidade, confianza e reputación.

Financiado por la Unión Europea NextGenerationEU
Plan de Recuperación, Transformación y Resiliencia
Gobierno de España · Ministerio de Industria y Turismo · Secretaría de Estado de Turismo
XUNTA DE GALICIA
Deputación DA CORUÑA

Un sector especialmente exposto

Datos Sensibles

Información persoal, preferencias, historiais, datos de pagamento en toda a cadea de valor.

Terciarización Alta

PMS, channel managers, OTAs, pasarelas, axencias incrementan o risco fóra do perímetro directo.

Que está en xogo

Consecuencias dunha brecha

Impacto Económico

Paradas, rescates, sancións, custos de peritaxe e recuperación directos.

Impacto Reputacional

Retroceso en intención de visita, aumento de reclamacións e reseñas negativas.

Impacto Operativo

Equipamentos bloqueados, procesos manuais de continxencia, descoordinación con socios.

Enfoque de Goberno

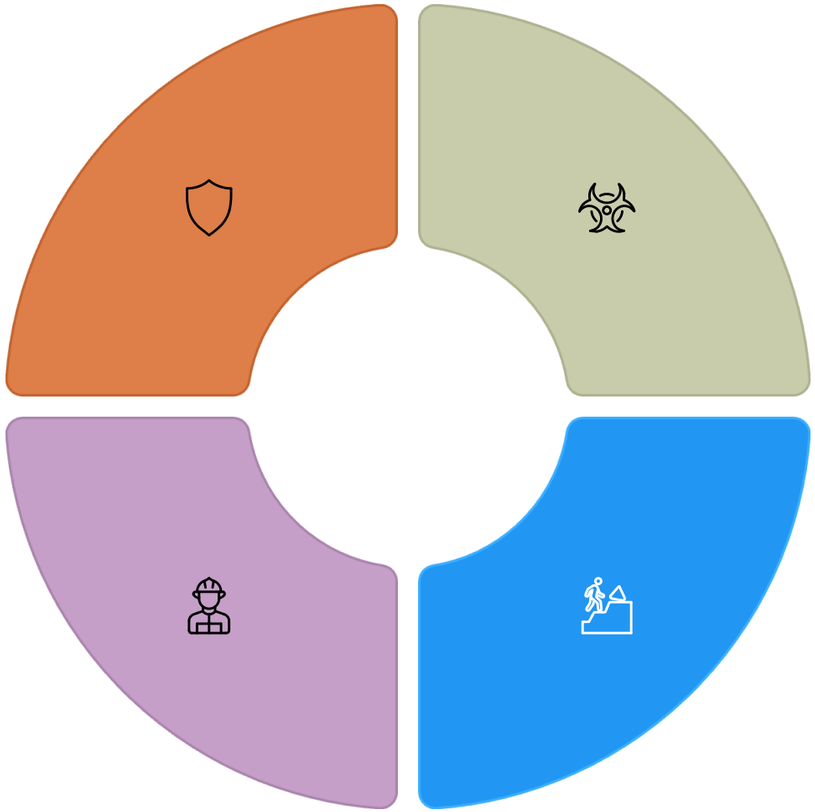
Non só tecnoloxía

Que Protexemos

Inventario de activos: datos, sistemas, procesos, localizacións, provedores.

De Que Protexemos

Modelo de amenazas: fraude, phishing, malware, exposición accidental.



Como Respondemos

Capacidade de resiliencia documentada con roles e procedementos.

Nivel de Risco

Criterios de avaliación e priorización por impacto.

Integrar a Ciberseguridade na Cultura e nas Rutinas

1

Concienciación Continua

Formación breve, simulacións de phishing, recordatorios de boas prácticas.

2

Roles e Mínimos

Coñecementos específicos por función: reservas, atención, redes sociais, datos.

3

Procesos Sinxelos

Facilitar o reporte de incidentes e solicitudes de acceso lexítimo.

Cadea de Subministro e Terceiros

O Eslabón Crítico

Gran parte do risco está fóra: solucións de reservas, email, marketing, axencias, integracións de pagamento e analítica.

Clasificación

Por criticidade do provedor.

Avaliación

Inicial e cláusulas contractuais.

Revisión

Periodica e plan de saída.

Datos e ciclo de vida

> ## Menos é Máis
>
> A protección empeza antes de almacenar nada. Reducir cantidade, delimitar finalidade e tempo, planificar eliminación ou anonimización.

Isto simplifica seguridade, reduce exposición e facilita cumprimento sen fricciónsinnecesarias.

Indicadores que Importan

Detección e resposta

Tempo medio de detección e resposta a incidentes.

Simulacións

Persoal que supera simulacións de phishing.

Parches Críticos

Tempo medio de aplicación de actualizacións.

Restauracións

Éxito en simulacros de recuperación.

Protección da Información

Defensas técnicas e organizativas eficaces para salvagardar datos sensibles e servicios críticos no sector turístico.

Firewalls e Seguridade Perimetral

Sistema de Filtros e Controis

NGFW e WAF

Firewall de nova xeración inspecciona tráfico por portos, aplicacións e patróns de ataque.

WAF protexe aplicacións web fronte a inxeccións SQL, XSS, forza bruta e bots.

Política "Denegar por Defecto"

Abrir unicamente portos/servicios indispensables e documentar cada excepción.

Inspección activa con módulos IPS/IDS e regras OWASP.

Que Implantar y Como Operarlo

Denegar por Defecto

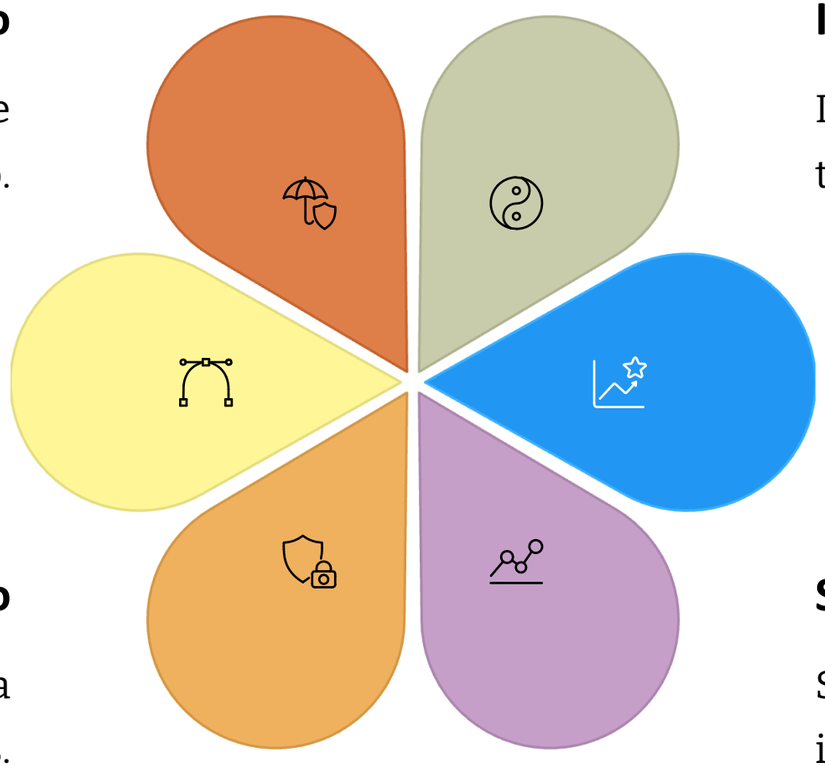
Só se permite o tráfico explicitamente autorizado.

Supervisión 24/7

Centralización de logs e alertas ante anomalías.

Acceso Seguro

VPN cifrada, MFA e IPs permitidas para administradores.



Inspección Activa

IPS/IDS detectan e bloquean ameazas en tempo real.

Anti-Bots e Taxa

Protección contra forza bruta e tráfico malicioso.

Segmentación Interna

Separación de redes con VLANs (oficina, invitados, IoT).

Encriptación de Datos

En Tránsito

Protexe a información mentres se move entre sistemas. Utiliza:

- HTTPS con TLS 1.2/1.3 e HSTS activo para a navegación web.
- VPN cifradas para garantir accesos remotos seguros.

En Repouso

Asegura os datos almacenados en calquera soporte. Implementa:

- Cifrado de bases de datos e volumes con AES-256.
- Xestión de claves con rotación periódica e segura.
- Contraseñas sempre hasheadas con algoritmos robustos como bcrypt o Argon2 con sal.
- Pagamentos con tokenización en pasarelas certificadas, evitando almacenar PAN/CVV.

Xestión de Certificados

Esencial para a confianza e a autenticación. Asegura:

- Adquisición e renovación automática de certificados SSL/TLS.
- Uso de Autoridades de Certificación (CA) de confianza.
- Monitoreo constante da validez e revocación de certificados.

Políticas de Seguridade Internas

Eixes mínimos de política

Autenticación e Contraseñas

MFA obrigatorio para tódolos accesos, uso de xestor corporativo e revocación inmediata de contas.

Parches e Vulnerabilidades

Actualizacións regulares e escaneos de seguridade para identificar e corrixir fallos proactivamente.

Higiene do Correo e Dominio

Filtros robustos anti-phishing/malware e concienciación constante sobre ameazas.

Mínimo Privilexio

Accesos estritamente basados en rol con caducidade e revisión periódica para limitar riscos.

Protección de Endpoints e Móbiles

Defensa de todos os dispositivos, con antivirus avanzado e prevención de perda de datos.

Ciclo de Desenvolvemento Seguro

Integrar a seguridade desde a concepción ata o despregamento de todo o software.

Procedementos Cotidianos

01

Onboarding/Offboarding

Checklist de permisos, dispositivos, claves e documentación.

02

Xestión de Incidentes

Canle simple de reporte, roles definidos, pasos de contención e simulacros periódicos.

03

Formación Continua

Cápsulas trimestrais de 10-15 minutos sobre phishing, nube, datos sensibles e mobilidade.

Xestión de accesos e copias de seguridade

Accesos

Inventario Vivo

Contas humanas e de servizo, SSO para centralizar altas/baixas e auditoría.

Alertas Intelixentes

Intentos repetidos de login, localizacións inusuais, creación de contas privilexiadas.

Rexistros de Acceso

En sistemas críticos conservados o tempo suficiente para análise.

Copias de Seguridade (Backups)

Regra 3-2-1

3

Copias

Manter tres copias dos datos.

2

Soportes

En dous soportes distintos.

1

Offline

Unha copia fóra da rede principal.

RTO e RPO

RTO

Recovery Time Objective: Tempo máximo de recuperación do servicio.

Definir e ensaiar regularmente.

RPO

Recovery Point Objective: Perda de datos tolerable.

Unha copia non restaurada non é fiable.

Seguridade en Wi-Fi

Redes Inalámbricas Seguras

Segmentación Estrita

Redes separadas: invitados, operación interna, IoT. Illamento cliente-cliente en rede de invitados.

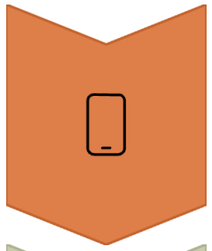
Autenticación Robusta

WPA3-Enterprise en red interna, rotación de claves PSK, deshabilitar WPS.

Monitorización

Detectar puntos de acceso rogue, limitar potencia, rexistrar accesos.

Dispositivos Móbiles e Kioscos



MDM Completo

Cifrado de disco, políticas de bloqueo, borrado remoto, restrición de apps.

Tabletas e Kioscos

Perfís restrinxidos, navegación limitada, sen almacenamento local de datos sensibles.

TPV e Pagamento

Rede separada, sen navegación á internet, mantemento documentado con provedor.