CAPACITACIÓN USACH
UNIVERSIDAD DE SANTIAGO DE CHILE

Gestión de Incidentes y Continuidad Operacional

Workshop N°3: Experiencias prácticas y aplicación con Ley Marco de Ciberseguridad

ALIGNMENT
SOLUCIONES ESTRATÉGICAS

DIPLOMADO
CIBERSEGURIDAD

Agenda

- Contexto de las funciones de Continuidad Operación y Gestión de Incidentes
- Conceptos claves de Continuidad Operación y Gestión de Incidentes
- Revisión del proceso de Gestión de Incidentes
- Revisión del proceso de Gestión de Continuidad Operativa
- Desafíos en la implementación de Ley Marco de Ciberseguridad

Profesor

Carlos Lobos de Medina

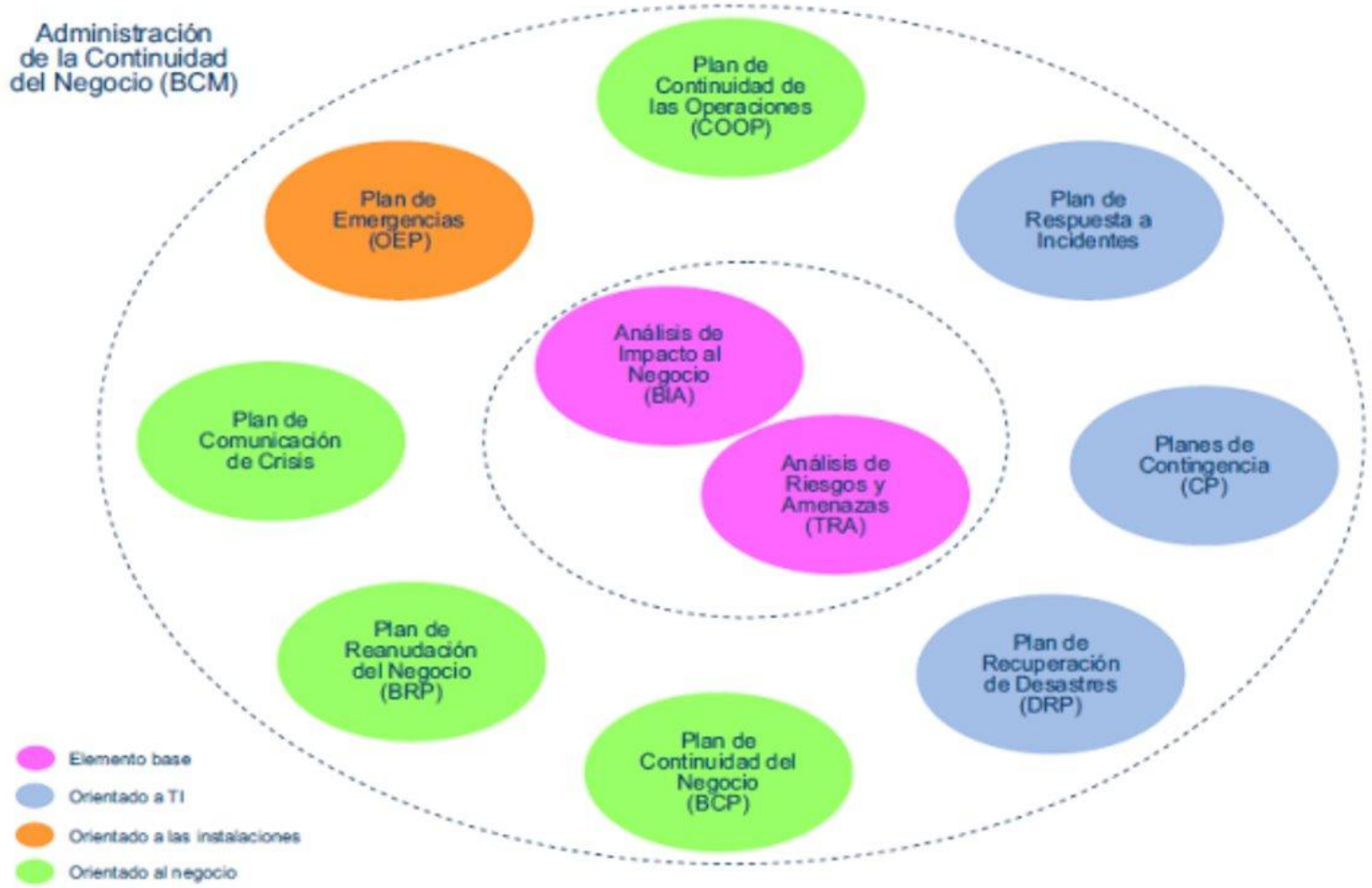
Ingeniero Civil en Informática y Magister en Informática © de la Universidad de Santiago de Chile, Diplomado en Auditoría de Sistemas, Postitulado en Seguridad Computacional de la Universidad de Chile.

Especialista en gobernanza, gestión y control de tecnologías de información empleando modelos como COBIT, ITIL, ISO 27001 e ISO 22301. Posee certificaciones internacionales CISA, CISM, COBIT, ISO Lead Auditor 27001, ISO Lead Auditor BS 25599 e ITIL V3, entre otras.}

https://www.linkedin.com/in/clobos/

Contexto de las funciones de Continuidad Operativa y Gestión de Incidentes

Actividades operativas en el Contexto



Son muchas las actividades y conceptos que surgen en un contexto de continuidad operativa y gestión de incidentes!!!!

Vamos a ver los conceptos claves, roles, responsabilidades y alcances para irlos entendiendo poco a poco!!

¿Qué riesgos nos impulsan a gestionar incidentes y continuidad operativa?

Emol

¿Qué pasó?: El fallo de Amazon Web Service que que desconectó apps, bancos y plataformas de todo el mundo

El problema registrado en uno de sus centros de datos de EE.UU. provocó una cadena de incidencias que se multiplicaron a lo largo del...

hace 2 semanas

Independent en Español

Falla en Amazon y Microsoft afecta bancos, vuelos y hasta Minecraft

Tanto Amazon como Microsoft enfrentaron este miércoles una interrupción importante en sus servicios de computación en la nube, lo que afectó...

hace 1 semana

WeLiveSecurity

Ataque ransomware al grupo GTD afecta organismos públicos y empresas de Chile y Perú

Ataque ransomware al grupo GTD afecta organismos públicos y empresas de Chile y Perú. El ransomware, conocido como Rorschach o BabLock, llama la...

06-11-2023

Bit Life Media

El ciberataque de ransomware a IFX Networks afecta a Colombia, Chile, Panamá y 762 empresas

El ciberataque de ransomware a IFX Networks afecta a decenas de servicios en Colombia, Chile, Panamá y a 762 empresas · Más de dos millones de...

15-09-2023

La Tercera

Hackeo al ISP: el ataque que tiene en jaque a Aduanas y mantiene en pausa servicios clave de salud

Desde el viernes el sitio web del organismo sigue caído y por ahora no hay una fecha clara para su reposición. Mientras tanto, para evitar...

01-07-2025

Emol

Prevención del Delito sufre ataque informático: Hay intermitencia en servicios virtuales

El episodio fue reportado este jueves y gatilló la activación del Protocolo de Seguridad para la Integridad de la Información.

11-09-2025

CNN Chile

Sernac inicia procedimiento con el Banco Santander por vulneración de datos personales durante ciberataque del 2024

El caso se remonta a mayo de 2024, cuando la información personal de cerca de cuatro millones de personas fue expuesta.

27-06-2025

Clarin.com

Cibercriminales aseguran tener datos del Ministerio de Salud y dan un plazo para publicarlos

Un grupo de atacantes publicó un posteo donde dicen poseer “información altamente sensible de 2 millones de pacientes en archivos de Excel”.

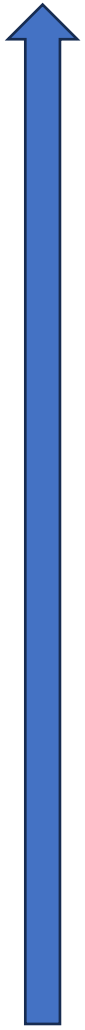
hace 3 semanas

¿Qué elementos de gestión son claves?

Estratégico

Gestión

Operativo



Gestión de Crisis (Alta Dirección)
Proceso coordinado de liderazgo, comunicación y toma de decisiones frente a eventos críticos que amenazan la estabilidad, reputación o continuidad de la organización, buscando restablecer el control y la confianza institucional.

Plan de Continuidad del Negocio (Procesos de Negocio)
Marco estratégico que asegura la operación de los procesos esenciales durante y después de una disrupción, protegiendo los recursos críticos, cumpliendo compromisos y garantizando la continuidad del servicio.

Plan de Recuperación de Incidentes (TI):
Conjunto de procedimientos técnicos diseñados para restaurar infraestructuras, sistemas y datos tras un evento disruptivo, asegurando la disponibilidad y funcionalidad de los servicios tecnológicos.

Plan de Respuesta a Incidentes (Ciberseguridad):
Guía estructurada que define cómo detectar, analizar, contener y erradicar amenazas digitales, minimizando impactos y fortaleciendo la resiliencia frente a ataques o vulneraciones de seguridad.

¿Qué tipo de problema, riesgo y tratamiento requiere?

Emol

¿Qué pasó?: El fallo de Amazon Web Service que que desconectó apps, bancos y plataformas de todo el mundo

El problema registrado en uno de sus centros de datos de EE.UU. provocó una cadena de incidencias que se multiplicaron a lo largo del...

hace 2 semanas

Independent en Español

Falla en Amazon y Microsoft afecta bancos, vuelos y hasta Minecraft

Tanto Amazon como Microsoft enfrentaron este miércoles una interrupción importante en sus servicios de computación en la nube, lo que afectó...

hace 1 semana

Caída de proveedores de servicios esenciales

Plan de respuesta a incidentes más en un foco proactivo e informativo, pero no con responsabilidad mayor en la contención y reanudación

Actividad	Rol Principal ante la caída de AWS	Acciones Clave que deben ejecutar
Gestión de Crisis	Liderar la toma de decisiones estratégicas y coordinar la respuesta institucional ante un evento crítico con alto impacto reputacional o de servicio.	- Activar el Comité de Crisis. - Evaluar impacto en clientes, reguladores y operaciones. - Aprobar mensajes oficiales y plan comunicacional. - Supervisar la ejecución de continuidad y recuperación. - Monitorear la evolución y declarar cierre de crisis.
Plan de Continuidad del Negocio (BCP)	Mantener operativos los procesos críticos a pesar de la indisponibilidad de AWS, usando estrategias alternativas.	- Identificar procesos afectados. - Activar sitios o servicios alternos. - Ejecutar planes manuales o de contingencia. - Asegurar comunicación interna y priorización de recursos. - Coordinar con TI y proveedores.
Plan de Recuperación de Incidentes (TI/DRP)	Restaurar la infraestructura tecnológica y los sistemas afectados por la caída del proveedor en el menor tiempo posible.	- Activar procedimientos de recuperación. - Conectar respaldos locales o en otra nube (multi-cloud, on-premise). - Validar integridad de datos. - Documentar tiempos de recuperación (RTO/RPO). - Informar avance al Comité de Crisis.
Plan de Respuesta a Incidentes (Ciberseguridad)	Verificar que la interrupción no esté asociada a un incidente de seguridad o ciberataque y mantener el monitoreo activo.	- Analizar si existe correlación con ataques DDoS o vulnerabilidades. - Asegurar registros de auditoría y alertas. - Notificar a CSIRT/CISO. - Contener riesgos secundarios (phishing, spoofing, accesos no autorizados). - Emitir informe técnico.

¿Qué tipo de problema, riesgo y tratamiento requiere?

WeLiveSecurity

Ataque ransomware al grupo GTD afecta organismos públicos y empresas de Chile y Perú

Ataque ransomware al grupo GTD afecta organismos públicos y empresas de Chile y Perú. El ransomware, conocido como Rorschach o BabLock, llama la...

06-11-2023

Bit Life Media

El ciberataque de ransomware a IFX Networks afecta a Colombia, Chile, Panamá y 762 empresas

El ciberataque de ransomware a IFX Networks afecta a decenas de servicios en Colombia, Chile, Panamá y a 762 empresas · Más de dos millones de...

15-09-2023

Ciberataques en proveedores de servicios esenciales

Plan de respuesta a incidentes más en un foco proactivo e informativo, **surge la necesidad de evaluar la exposición de datos personales.**

Actividad	Rol Principal ante la caída de GTD e IFX	Acciones Clave que deben ejecutar
Gestión de Crisis	Coordinar la respuesta estratégica, comunicacional y reputacional ante la pérdida de servicios de seguridad y conectividad críticos, manteniendo el control institucional y la confianza de las partes interesadas.	- Activar el Comité de Crisis. - Evaluar impacto operativo, financiero y reputacional. - Comunicar a Alta Dirección y partes interesadas. - Aprobar mensajes oficiales. - Monitorear evolución del evento y declarar cierre de crisis.
Plan de Continuidad del Negocio (BCP)	Asegurar la operación mínima de los procesos esenciales mientras los proveedores restablecen sus servicios, activando estrategias de respaldo y continuidad manual.	- Identificar procesos críticos afectados (red, SOC, monitoreo, conectividad). - Activar proveedores o enlaces alternativos. - Aplicar procedimientos manuales de contingencia. - Coordinar acciones entre áreas operativas y TI. - Documentar brechas y lecciones aprendidas.
Plan de Recuperación de Incidentes (TI/DRP)	Restablecer la infraestructura tecnológica y servicios asociados mediante planes de recuperación locales o en nubes alternas, minimizando la interrupción.	- Ejecutar restauración desde respaldos. - Activar datacenters secundarios o soluciones multi-cloud. - Validar integridad de datos y servicios. - Registrar tiempos de recuperación (RTO/RPO). - Coordinar con GTD e IFX la reintegración técnica.
Plan de Respuesta a Incidentes (Ciberseguridad)	Detectar si la caída obedece a un ataque o compromiso de seguridad, y proteger los entornos internos de posibles efectos colaterales.	- Revisar correlaciones de alertas y logs. - Contactar al CSIRT nacional o sectorial. - Fortalecer monitoreo con SOC interno o alterno. - Aislar sistemas vulnerables. - Emitir reporte técnico y lecciones aprendidas.
Respuesta a Incidentes de Privacidad (Protección de Datos)	Proteger los datos personales ante la posible exposición, pérdida o acceso indebido derivados de la interrupción o falla de los proveedores.	- Verificar si existe afectación de datos personales. - Activar protocolo de notificación a la autoridad o titulares. - Coordinar con el Oficial de Cumplimiento y DPO. - Documentar medidas de mitigación. - Evaluar cumplimiento ISO 27701 y Ley 19.628.

¿Qué tipo de problema, riesgo y tratamiento requiere?

La Tercera

Hackeo al ISP: el ataque que tiene en jaque a Aduanas y mantiene en pausa servicios clave de salud

Desde el viernes el sitio web del organismo sigue caído y por ahora no hay una fecha clara para su reposición. Mientras tanto, para evitar...

01-07-2025

Emol

Prevención del Delito sufre ataque informático: Hay intermitencia en servicios virtuales

El episodio fue reportado este jueves y gatilló la activación del Protocolo de Seguridad para la Integridad de la Información.

11-09-2025

Ciberataques reales (Ransomware) en las organizaciones

Plan de respuesta a incidentes activo y critico, siendo el motor clave de la contención, recuperación y activación.

Actividad	Rol Principal ante el ataque de ransomware	Acciones Clave que deben ejecutar
Gestión de Crisis	Dirigir la respuesta institucional ante un evento de alto impacto público y mediático, asegurando decisiones rápidas, coordinación interinstitucional y comunicación transparente.	- Activar Comité de Crisis. - Evaluar impacto reputacional, operacional y político. - Comunicar a autoridades superiores y ciudadanía. - Establecer vocería oficial. - Supervisar ejecución de continuidad, ciberseguridad y privacidad. - Gestionar relación con prensa y CSIRT Gobierno.
Plan de Continuidad del Negocio (BCP)	Mantener la operatividad de los servicios esenciales de salud pública y atención ciudadana, incluso con sistemas comprometidos.	- Identificar procesos críticos manualizables (laboratorio, denuncias, reportes). - Activar procedimientos alternos sin depender de sistemas afectados. - Coordinar apoyo interinstitucional (Ministerio, CSIRT, Subtel). - Garantizar comunicación interna continua. - Priorizar funciones esenciales de atención pública.
Plan de Recuperación de Incidentes (TI/DRP)	Restaurar servicios tecnológicos y sistemas comprometidos por el ransomware, garantizando integridad de la información y disponibilidad segura.	- Aislar servidores afectados. - Recuperar desde respaldos verificados. - Reinstalar infraestructura crítica y actualizar parches. - Validar limpieza de entornos antes de reconexión. - Documentar tiempos de recuperación (RTO/RPO).
Plan de Respuesta a Incidentes (Ciberseguridad)	Detectar, contener y erradicar la amenaza, evitando propagación lateral y pérdida de datos, en coordinación con el CSIRT Nacional.	- Identificar vector de ataque y tipo de ransomware. - Cortar comunicaciones externas sospechosas. - Preservar evidencias y registros. - Reforzar monitoreo SIEM/SOC. - Implementar medidas de contención y notificación a CERT/CSIRT. - Analizar lecciones aprendidas y vulnerabilidades explotadas.
Respuesta a Incidentes de Privacidad (Protección de Datos)	Proteger los datos personales y sensibles afectados por el cifrado o posible exfiltración, cumpliendo las obligaciones de transparencia y notificación.	- Evaluar si hubo filtración de datos personales o clínicos. - Activar protocolo de notificación a la autoridad y titulares. - Coordinar con el DPO y Oficial de Cumplimiento. - Implementar medidas de mitigación (bloqueo, monitoreo de fugas). - Comunicar medidas preventivas a los afectados. - Documentar trazabilidad y acciones conforme a ISO 27701.

¿Qué tipo de problema, riesgo y tratamiento requiere?

La Tercera

Hackeo al ISP: el ataque que tiene en jaque a Aduanas y mantiene en pausa servicios clave de salud

Desde el viernes el sitio web del organismo sigue caído y por ahora no hay una fecha clara para su reposición. Mientras tanto, para evitar...

01-07-2025

Emol

Prevención del Delito sufre ataque informático: Hay intermitencia en servicios virtuales

El episodio fue reportado este jueves y gatilló la activación del Protocolo de Seguridad para la Integridad de la Información.

11-09-2025

Exfiltraciones de Datos Personales de alta sensibilidad

Respuesta a incidentes de privacidad toma un rol activo y critico, siendo el actividades de notificación y evaluación del impacto de privacidad, así como actividades de reparación y contención.

Actividad	Rol Principal ante la exfiltración de datos personales	Acciones Clave que deben ejecutar
Gestión de Crisis	Liderar la respuesta estratégica y comunicacional ante un evento de alta sensibilidad pública, asegurando transparencia, coordinación institucional y control reputacional.	- Activar Comité de Crisis y convocar Alta Dirección. - Evaluar impacto en clientes, pacientes y reguladores. - Establecer vocería oficial y comunicación responsable. - Coordinar con áreas legales, TI y cumplimiento. - Supervisar ejecución de planes técnicos y de privacidad. - Mantener trazabilidad y control de información pública.
Plan de Continuidad del Negocio (BCP)	Asegurar la continuidad de los servicios financieros o clínicos mientras se aíslan los sistemas comprometidos y se implementan medidas de contención.	- Identificar procesos críticos afectados por el incidente. - Mantener operación con entornos seguros o alternativos. - Coordinar continuidad con áreas funcionales clave. - Establecer procedimientos manuales o provisionales. - Monitorear estabilidad operativa y comunicación a usuarios.
Plan de Recuperación de Incidentes (TI/DRP)	Restaurar los sistemas comprometidos, reforzando las medidas de seguridad y garantizando la integridad de la infraestructura tecnológica.	- Aislar entornos comprometidos. - Cambiar credenciales y accesos de proveedores externos. - Verificar integridad de respaldos y bases de datos. - Implementar parches y controles de acceso reforzados. - Validar recuperación segura de sistemas y registros.
Plan de Respuesta a Incidentes (Ciberseguridad)	Contener y erradicar la amenaza que permitió la filtración, identificando vulnerabilidades, actores y rutas de fuga de información.	- Analizar logs y detectar puntos de exfiltración. - Coordinar con CSIRT, CERT o equipos forenses. - Implementar bloqueo de canales de fuga (FTP, nube, VPN). - Monitorear redes internas y externas. - Elaborar informe técnico con causas raíz y medidas correctivas.
Respuesta a Incidentes de Privacidad (Protección de Datos)	Mitigar el impacto legal y ético de la filtración de datos personales, cumpliendo las obligaciones de notificación y transparencia.	- Activar protocolo de notificación a la autoridad (AEPD, AAIP, etc.). - Notificar a los titulares de los datos afectados. - Coordinar con el DPO y áreas de cumplimiento. - Documentar evaluación de impacto (DPIA). - Implementar medidas de reparación y contención. - Comunicar compromiso de mejora y seguridad futura.

¿Qué podemos sacar en limpio desde estas experiencias?

1 Gestión de Crisis: Liderazgo y Dirección Estratégica

Coordina la toma de decisiones, define prioridades y comunica oficialmente.

Su función es mantener el control institucional, la reputación y la confianza pública.

2 Continuidad del Negocio: Mantener la Operación Crítica

Asegura que los procesos esenciales sigan funcionando, incluso en disrupción.

Activa planes alternativos, procedimientos manuales y recursos de respaldo.

3 Recuperación de Incidentes (TI): Restaurar Infraestructura y Servicios

Ejecuta la recuperación técnica tras fallas, ataques o caídas de proveedores.

Restaura sistemas, bases de datos y comunicaciones cumpliendo RTO/RPO definidos.

4 Respuesta a Incidentes (Ciberseguridad): Contención y Erradicación

Detecta, contiene y elimina la amenaza antes de que escale.

Preserva evidencias, coordina con el CSIRT y refuerza controles de seguridad.

5 Respuesta a Incidentes de Privacidad: Cumplimiento y Transparencia

Evalúa el impacto sobre los datos personales y cumple con las obligaciones legales.

Notifica a autoridades y titulares, mitigando el daño y protegiendo la confianza pública.

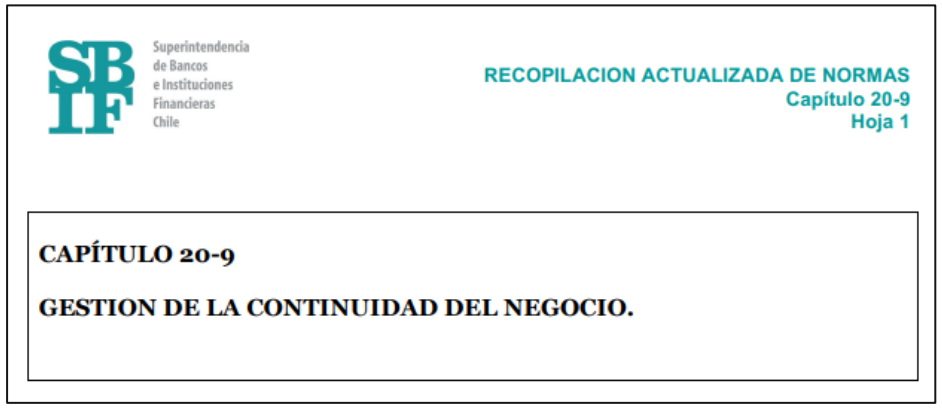
6 Coordinación Integral: El Factor Decisivo del Éxito

La respuesta efectiva depende de la sincronización entre CISO, CIO, DPO y Alta Dirección.

El liderazgo y la colaboración superan la crisis más rápido que la tecnología por sí sola.

¿Podríamos ser exitosos frente a alguno de los incidentes vistos si no tenemos competencias, nos preparamos adecuadamente y ejercitamos estas definiciones?

Pero…. Hay mucho más en continuidad operativa


Superintendencia de Bancos e Instituciones Financieras Chile

RECOPILACION ACTUALIZADA DE NORMAS
Capítulo 20-9
Hoja 1

CAPÍTULO 20-9

GESTION DE LA CONTINUIDAD DEL NEGOCIO.

- La entidad considera como mínimo los escenarios de contingencia referidos a: la falta total y parcial de los **sistemas tecnológicos; ataques maliciosos que afecten la ciberseguridad; la ausencia de personal crítico; la imposibilidad de acceder y/o utilizar las instalaciones físicas y la falta de provisión de los servicios críticos contratados a proveedores.**

RAN 20-9 - Normativa Financiera en Chile

- Cualquier incidente de ciberseguridad materializado y de cierto grado de magnitud requiera articularse con DRP, BCP e incluso la gestión de crisis.

- Pero pueden existir muchos elementos fuera de incidentes de ciberseguridad que requieran desarrollar una continuidad operativa.

Desastres naturales – Terremotos por ejemplo

Terremotos o Desastres Naturales

Los problemas críticos se ven a nivel de BCP y Gestión de Crisis, a menos que tus instalaciones se vean gravemente afectadas.

Actividad	Rol Principal ante un terremoto o desastre natural	Acciones Clave que deben ejecutar
Gestión de Crisis	Liderar la respuesta estratégica y la coordinación institucional frente a un evento de alto impacto humano, operativo y comunicacional.	- Activar el Comité de Crisis. - Evaluar daños humanos, operativos y logísticos. - Coordinar comunicación con autoridades, clientes y prensa. - Priorizar seguridad del personal y continuidad de servicios. - Tomar decisiones sobre cierre o traslado de operaciones. - Supervisar ejecución de los planes de continuidad y recuperación.
Plan de Continuidad del Negocio (BCP)	Garantizar que los procesos críticos sigan funcionando o sean restablecidos en el menor tiempo posible, pese a daños físicos o cortes de servicios.	- Activar sitios alternos o centros de respaldo. - Ejecutar procedimientos manuales para funciones críticas. - Coordinar con proveedores y aliados estratégicos. - Monitorear recursos vitales (energía, conectividad, transporte). - Priorizar servicios esenciales y atención a usuarios críticos. - Documentar brechas y resultados post-evento.
Plan de Recuperación de Incidentes (TI/DRP)	Restaurar la infraestructura tecnológica afectada por daños físicos, cortes eléctricos o pérdida de conectividad.	- Activar recuperación en datacenter secundario o nube. - Restablecer conectividad con sitios alternos. - Validar integridad de respaldos y sistemas esenciales. - Reemplazar equipamiento dañado y actualizar configuraciones. - Documentar tiempos de recuperación (RTO/RPO).
Plan de Respuesta a Incidentes (Ciberseguridad)	Asegurar que el entorno de crisis no sea aprovechado por atacantes o se generen nuevas vulnerabilidades durante la restauración.	- Intensificar monitoreo de seguridad ante intentos de intrusión. - Revisar logs y alertas por accesos no autorizados. - Coordinar con CSIRT nacional o sectorial. - Asegurar canales seguros de comunicación y acceso remoto. - Proteger respaldos de manipulación o sabotaje digital.

Cortes de luz generalizados – Efectos en transportes y las personas

Cortes de Luz Generalizado

Los problemas críticos se ven a nivel de BCP y Gestión de Crisis, menor medida DRP por faltas de UPS y generadores… otro factor importante la ausencia de personal critico.

Actividad	Rol Principal ante la caída de servicios críticos (luz, transporte, etc.)	Acciones Clave que deben ejecutar
Gestión de Crisis	Dirigir la respuesta organizacional ante un evento que afecta a personas, infraestructura y servicios esenciales, asegurando decisiones humanas y coordinadas.	- Activar el Comité de Crisis y priorizar la seguridad del personal. - Evaluar el impacto en instalaciones, colaboradores y operaciones críticas. - Comunicar lineamientos claros: asistencia, horarios, trabajo remoto o suspensión. - Coordinar con autoridades, servicios de emergencia y empresas proveedoras. - Mantener información confiable y apoyo emocional interno. - Supervisar la continuidad de funciones esenciales.
Plan de Continuidad del Negocio (BCP)	Mantener las funciones críticas operativas, adaptando procesos ante la falta de electricidad, conectividad o movilidad.	- Activar protocolos de contingencia por pérdida de energía o transporte. - Priorizar procesos esenciales (pagos, atención, soporte). - Establecer turnos flexibles o teletrabajo temporal. - Coordinar con RRHH medidas de contención y apoyo. - Garantizar condiciones básicas de seguridad y bienestar. - Documentar la efectividad de las medidas adoptadas.
Plan de Recuperación de Incidentes (TI/DRP)	Restaurar gradualmente los servicios tecnológicos una vez restablecida la energía o conectividad, asegurando integridad y estabilidad.	- Validar equipos tras cortes eléctricos prolongados. - Verificar servidores, UPS y redes antes de reconexión. - Activar respaldos en nubes o datacenters secundarios. - Documentar interrupciones y tiempos de recuperación. - Coordinar pruebas de sistemas antes de volver a producción.
Plan de Respuesta a Incidentes (Ciberseguridad)	Proteger la infraestructura digital ante vulnerabilidades generadas por la contingencia o restablecimientos abruptos.	- Monitorear accesos anómalos durante interrupciones o reconexiones. - Asegurar configuraciones y sistemas críticos tras apagones. - Evitar uso de redes o dispositivos no verificados. - Coordinar con CSIRT o equipos de respuesta. - Aumentar vigilancia frente a phishing o ingeniería social en periodos de caos.

Conceptos Claves de Incidentes

Las empresas en mayor o menor medida se preparan.

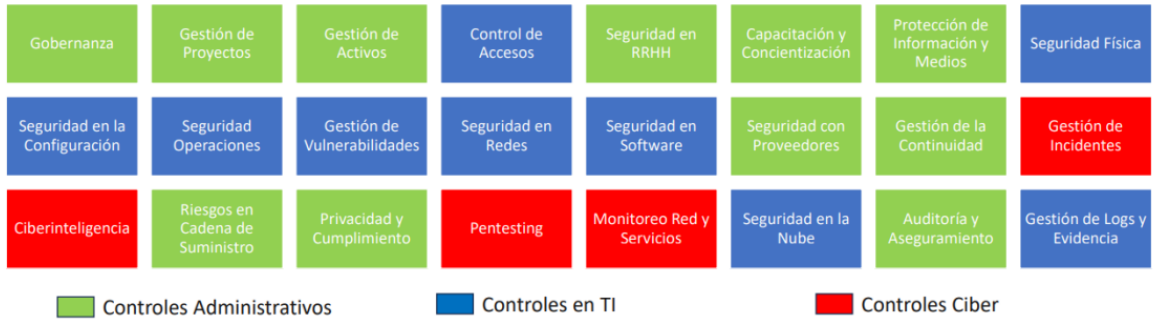
International Organization for Standardization
ISO
27002

CIS Controls
Version 8

01	Inventory and Control of Enterprise Assets
02	Inventory and Control of Software Assets
03	Data Protection
04	Secure Configuration of Enterprise Assets and
05	Account Management
06	Access Control Management
07	Continuous Vulnerability Management
08	Audit Log Management
09	Email and Web Browser Protections
10	Malware Defenses
11	Data Recovery
12	Network Infrastructure Management
13	Network Monitoring and Defense
14	Security Awareness and Skills Training
15	Service Provider Management
16	Application Software Security
17	Incident Response Management
18	Penetration Testing

MITRE ATT&CK™

De alguna manera u otra las empresa buscan desarrollara elementos para gestionar sus riesgos y establecer elementos de control…… **que ocurre si estos fallan?**



Naturaleza de los controles: NIST CSF y CIS Control

Función	Categoría	Identificador de Categoría
Gobernar (GV)	Contexto organizativo	GV.OC
	Estrategia de gestión de riesgos	GV.RM
	Funciones, responsabilidades y autoridades	GV.RR
	Política	GV.PO
	Supervisión	GV.OV
	Gestión de riesgos de la cadena de suministro en materia de seguridad cibernética	GV.SC
Identificar (ID)	Gestión de activos	ID.AM
	Evaluación de riesgos	ID.RA
	Mejora	ID.IM
Proteger (PR)	Gestión de identidades, autenticación y control de acceso	PR.AA
	Concienciación y capacitación	PR.AT
	Seguridad de datos	PR.DS
	Seguridad de plataformas	PR.PS
	Resistencia de la infraestructura tecnológica	PR.IR
Detectar (DE)	Monitoreo continuo	DE.CM
	Análisis de eventos adversos	DE.AE
Responder (RS)	Gestión de incidentes	RS.MA
	Análisis de incidentes	RS.AN
	Notificación y comunicación de la respuesta al incidente	RS.CO
	Mitigación de incidentes	RS.MI
Recuperar (RC)	Ejecución del Plan de Recuperación de Incidentes	RC.RP
	Comunicación de la recuperación del incidente	RC.CO

Cuando los controles de prevención y detección son sobrepasados necesitamos **capacidades de respuesta y recuperación.**

17.1	**Designar personal para administrar el manejo de incidentes**	N/A	Responder	●	●	●
	Designe una persona clave, y al menos una persona como respaldo, que gestionará el proceso de gestión de incidentes de la empresa. El personal de administración es responsable de la coordinación y documentación de la respuesta a incidentes y los esfuerzos de recuperación y puede consistir en empleados internos de la empresa, proveedores externos o un enfoque híbrido. Si utiliza un proveedor externo, designe al menos una persona interna de la empresa para supervisar cualquier trabajo de terceros. Revise anualmente o cuando ocurran cambios importantes en la empresa que puedan afectar esta protección.					
17.2	**Establecer y mantener información de contacto para informar incidentes de seguridad**	N/A	Responder	●	●	●
	Establecer y mantener la información de contacto de las partes que necesitan ser informadas de incidentes de seguridad. Los contactos pueden incluir personal interno, proveedores externos, fuerzas del orden, proveedores de seguros cibernéticos, agencias gubernamentales relevantes, socios del Centro de Intercambio y Análisis de Información (ISAC) u otras partes interesadas. Verificar los contactos anualmente para asegurarse de que la información está actualizada.					
17.3	**Establecer y mantener un proceso empresarial para informar de incidentes**	N/A	Responder	●	●	●
	Establezca y mantenga un proceso de la empresa para que la plana laboral informe de incidentes de seguridad. El proceso incluye el plazo de presentación de informes, el personal al que informar, el mecanismo de presentación de informes y la información mínima que se debe informar. Asegúrese de que el proceso esté disponible públicamente para toda la plana laboral. Revisar esta salvaguarda anualmente, o cuando se produzcan cambios significativos en la empresa que puedan afectar a esta Salvaguarda.					
17.4	**Establecer y mantener un proceso de respuesta a incidentes**	N/A	Responder		●	●
	Establezca y mantenga un proceso de respuesta a incidentes que aborde los roles y responsabilidades, los requisitos de cumplimiento y un plan de comunicación. Revise anualmente o cuando ocurran cambios importantes en la empresa que puedan afectar esta salvaguarda.					
17.5	**Asignar Roles Claves y Responsabilidades**	N/A	Responder		●	●
	Asigne roles claves y responsabilidades responder a incidentes, incluido el personal de legal, TI, seguridad de la información, instalaciones, relaciones públicas, recursos humanos, personal de respuesta a incidentes y analistas, según corresponda. Revise esta salvaguarda anualmente o cuando ocurran cambios importantes en la empresa que puedan afectar esta protección.					
17.6	**Definir mecanismos de comunicación durante la respuesta a incidentes**	N/A	Responder		●	●
	Determine qué mecanismos principales y secundarios se usarán para comunicarse e informar durante un incidente de seguridad. Los mecanismos pueden incluir llamadas telefónicas, correos electrónicos o cartas. Tenga en cuenta que ciertos mecanismos, como los correos electrónicos, pueden verse afectados durante un incidente de seguridad. Revisar anualmente, o cuando se produzcan cambios significativos en la empresa que puedan afectar a esta Salvaguarda.					
17.7	**Realizar ejercicios rutinarios de respuesta a incidentes**	N/A	Recuperar		●	●
	Planifique y lleve a cabo ejercicios y escenarios de respuesta a incidentes de rutina para el personal clave involucrado en el proceso de respuesta a incidentes a fin de prepararse para responder a incidentes del mundo real. Los ejercicios deben probar los canales de comunicación, la toma de decisiones y los flujos de trabajo. Realice pruebas anualmente, como mínimo.					
17.8	**Realizar revisiones posteriores a un incidente**	N/A	Recuperar		●	●
	Realice revisiones posteriores al incidente. Las revisiones posteriores al incidente ayudan a prevenir la repetición del incidente mediante la identificación de lecciones aprendidas y acciones de seguimiento.					

Controles de Gestión de Incidentes ISO 27002

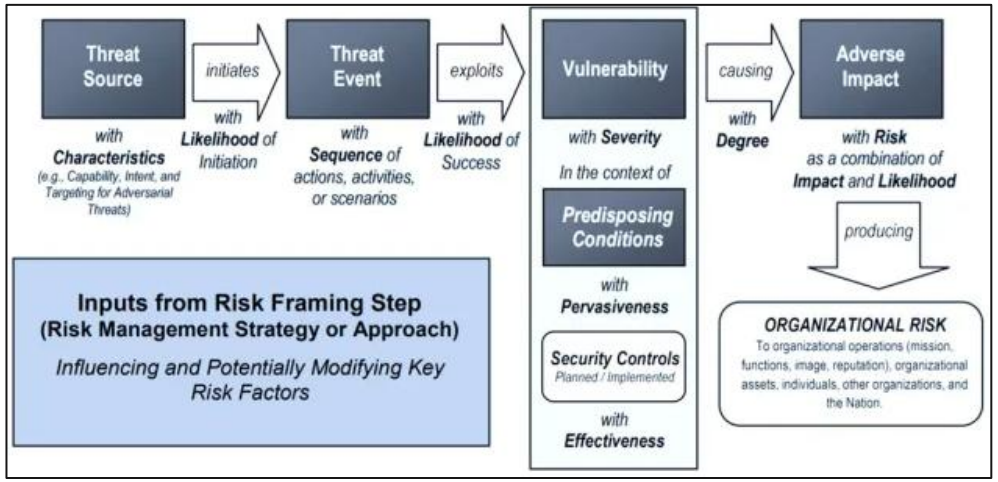
Control	Nombre del Control	Tipo de Controles	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
5,24	Responsabilidades y procedimientos	#Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Responder #Recuperar	#Información_seguridad_gestión_de_eventos	#Defensa
5,25	Evaluación y decisión sobre los eventos de seguridad de información	#Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar #Responder	#Información_seguridad_gestión_de_eventos	#Defensa
5,26	Respuesta a incidentes de seguridad de la información	#Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Responder #Recuperar	#Información_seguridad_gestión_de_eventos	#Defensa
5,27	Aprendizaje de los incidentes de seguridad de la información	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Identificar	#Información_seguridad_gestión_de_eventos	#Defensa
5,28	Recopilación de evidencias	#Detectivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar #Responder	#Información_seguridad_gestión_de_eventos	#Defensa
6,80	Reporte de eventos de seguridad de la información	#Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar	#Información_seguridad_gestión_de_eventos	#Defensa

- Desarrollar la capacidad de responder resulta clave frente a un incidente de ciberseguridad!!!

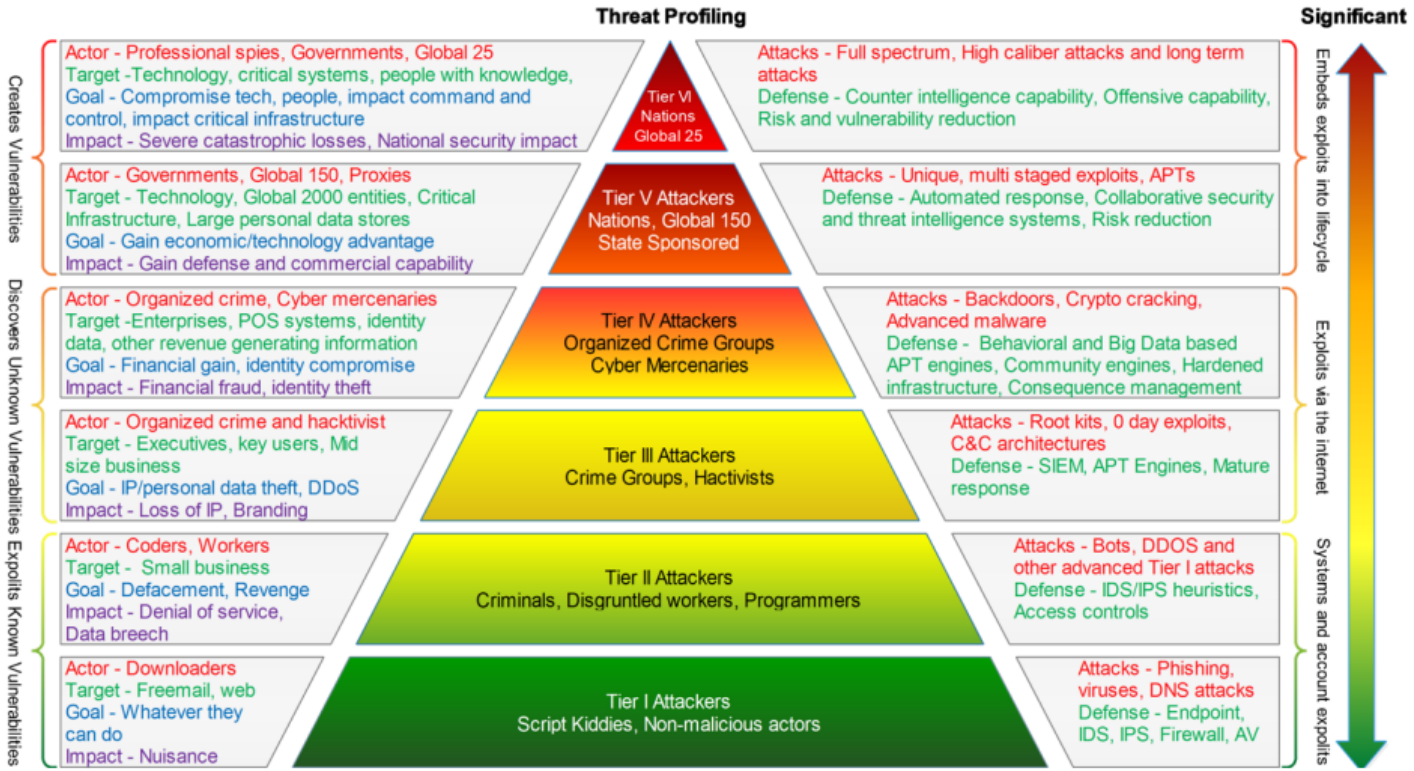
Taxonomía de un Incidente

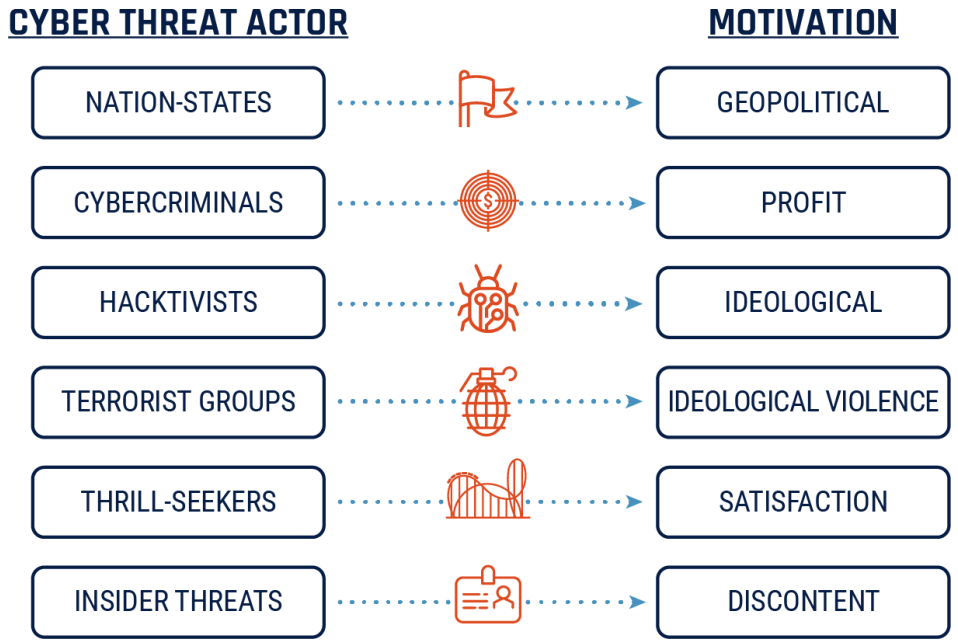
- Cyber Criminales emplean diversas Tácticas, Técnicas y Procedimientos (TTP) para desplegar amenazas que explotan vulnerabilidades en las organizaciones provocando un impacto adverso (riesgo organizacional)

- ¿Qué relación tienen las incidencias con los riesgos?



Categorizando amenazas y grupos criminales





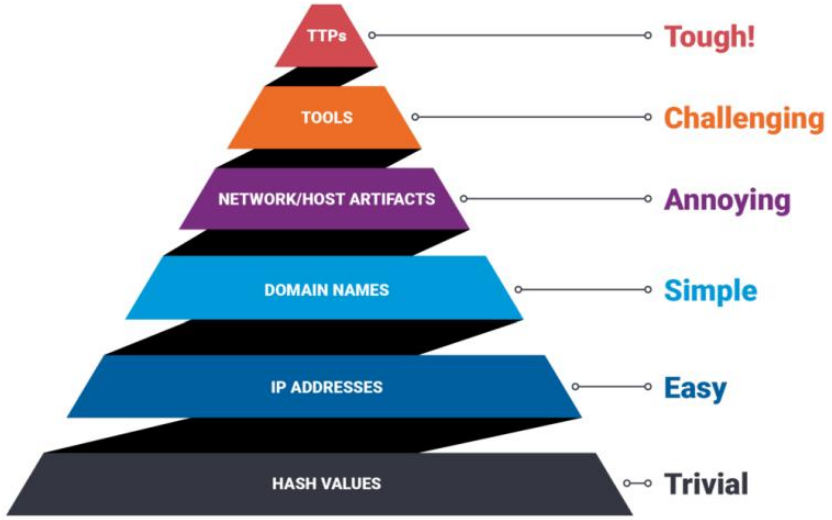
- Los diversos grupos criminales poseen diversas motivaciones y son capaces de emplear técnicas en diversos niveles, pero por muy sofisticados que sean explotaran vulnerabilidades de las más sencillas.

Grupos Criminales más activos

Grupo / Alias	Origen estimado	Tipo de actividad	TTPs más utilizadas (MITRE ATT&CK)	Países más afectados	Sectores más atacados
TA505 / Clop	Europa del Este	Ransomware y exfiltración de datos	T1566 (Phishing) T1190 (Exploiting Public Apps) T1041 (Data Exfiltration) T1486 (Encrypt Data for Impact)	Chile, México, Brasil, Argentina	Banca, retail, sector público
FIN12 / UNC1878	Rusia / Ucrania	Ransomware-as-a-Service (Ryuk/Conti)	T1078 (Valid Accounts) T1059 (PowerShell) T1105 (Exfiltration over Web Services) T1486 (Encryption)	Brasil, México, Ecuador	Salud, educación, seguros
Lapsus$ Group	Brasil / Reino Unido	Secuestro de datos y exposición mediática	T1534 (Internal Spearphishing) T1071 (Web Protocols) T1098 (Account Manipulation) T1562 (Defense Evasion)	Brasil, Chile, Ecuador, Colombia	Telecomunicaciones, tecnología, gobierno
RansomHouse	Europa del Este	Extorsión y robo de información	T1078 (Valid Accounts) T1021 (Remote Services) T1041 (Data Exfiltration) T1562 (Disable Security Tools)	Chile, Perú, México	Banca, energía, sector público
BlackCat / ALPHV	Rusia	Ransomware sofisticado (Rust)	T1569 (Service Execution) T1078 (Compromised Credentials) T1486 (Encryption) T1027 (Obfuscated Files)	Brasil, Chile, México	Energía, manufactura, gobierno
LockBit 3.0	Rusia / afiliados globales	Ransomware modular	T1059 (Command Shell) T1490 (Inhibit System Recovery) T1041 (Exfiltration) T1486 (Encryption)	México, Brasil, Chile, Argentina	Salud, finanzas, transporte
Hive / Hunters International	Europa del Este	Ransomware-as-a-Service	T1133 (External Remote Services) T1070 (Indicator Removal) T1569 (Execution) T1490 (System Recovery Inhibit)	Brasil, Ecuador, Panamá	Hospitales, finanzas, educación
Moses Staff	Oriente Medio	Sabotaje político y ciberespionaje	T1190 (Exploit Web Apps) T1498 (Network Denial of Service) T1485 (Data Destruction) T1105 (Command & Control)	Chile, Colombia, Costa Rica	Gobierno, defensa, energía

Fuente: Elaboración propia a partir de informes de Mandiant, CrowdStrike, Microsoft, Kaspersky, ESET, Fortinet, Interpol y CSIRT LATAM (2024–2025).

Pirámide del Dolor

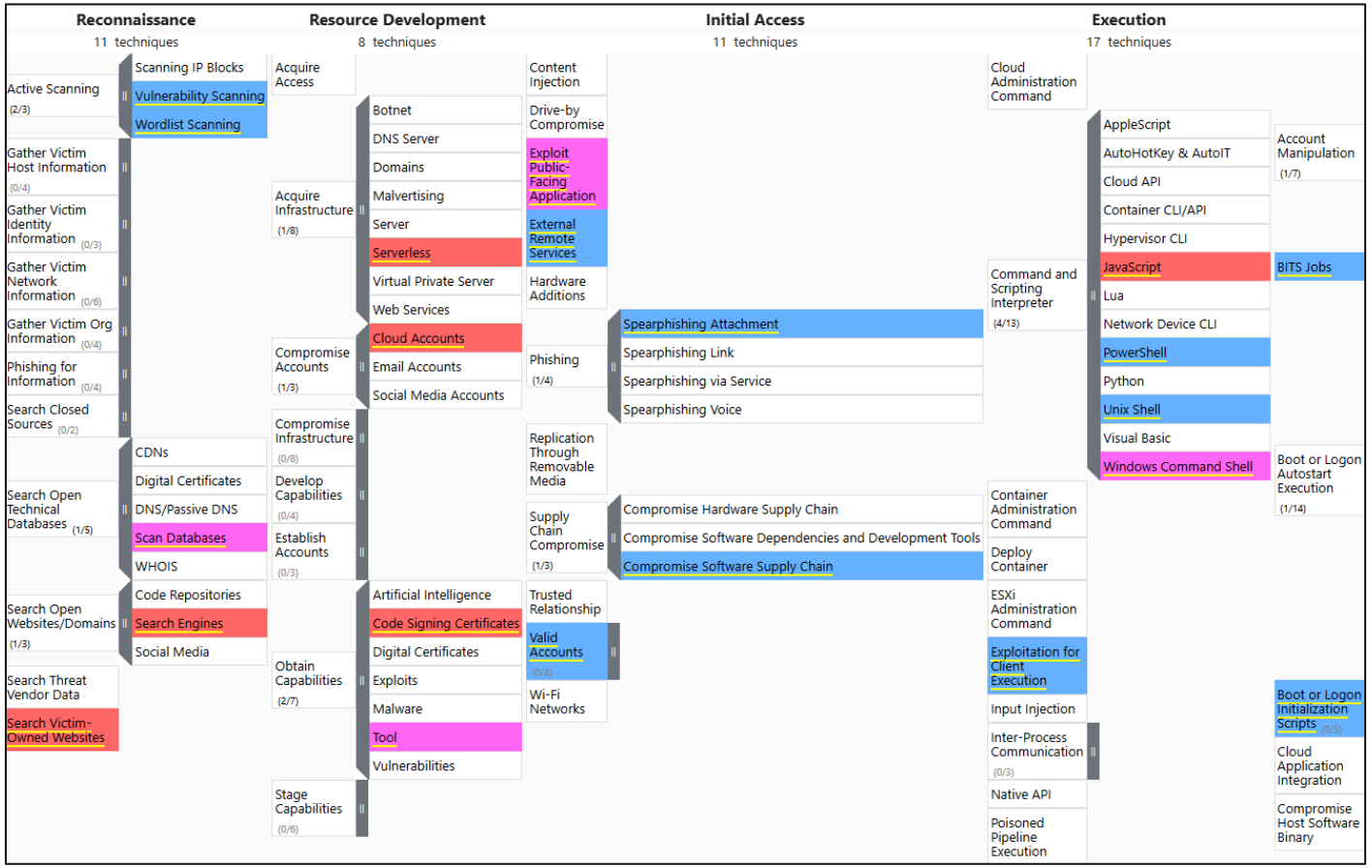


Nivel	Indicador	Ejemplo	Qué tan fácil puede cambiarlo el atacante	Dolor causado al atacante
Tácticas, Técnicas y Procedimientos (TTPs)	Comportamientos y métodos operativos del atacante	Uso de `PowerShell`, `WMIC`, `RDP`, `schtasks` para movimiento lateral o persistencia	Muy difícil — requiere rediseñar completamente la forma de atacar y entrenar al equipo	Muy alto
Artefactos de red / host	Huellas detectables en sistemas o redes	Rutas, nombres de archivos (`svc.exe`), claves de registro, cadenas en scripts	Difícil — implica reescribir herramientas y modificar patrones	Alto
Nombres de dominio	Infraestructura visible de comando y control (C2)	`update-secure.com`, `login-portal.net`	Moderado — necesita registrar nuevos dominios, configurar DNS y certificados	Medio
Direcciones IP	Servidores de control o exfiltración	`45.83.21.110`	Fácil — puede usar otros proxies, VPN o infraestructura comprometida	Bajo
Hash de archivo	Identificador único del malware o herramienta usada	`SHA256: a32f8d...`	Muy fácil — basta recompilar o modificar el archivo	Muy bajo

- La mejor ciberdefensa es la que conoce el comportamiento de los adversarios (cibercriminales)
- Pero no descartar ningún otro método, son complementarios

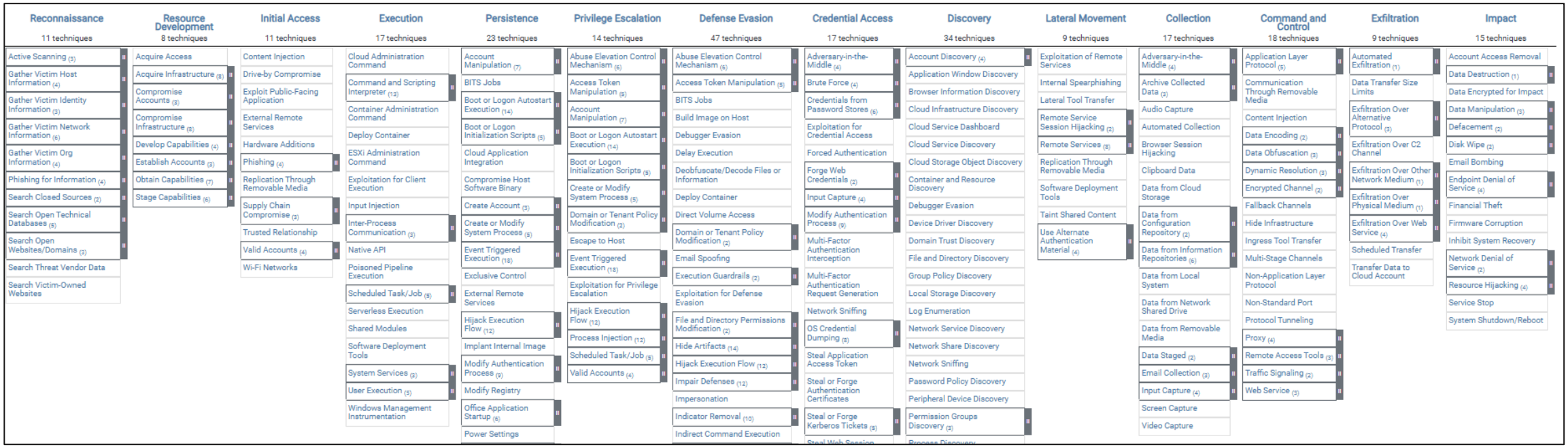
MITRE ATT&CK y los TTP

- MITRE ATT&CK es un marco público que mapea las tácticas y técnicas reales usadas por adversarios para facilitar la detección y defensa.
- Sirve como lenguaje común para ciberdefensa, threat hunting y red teams, permitiendo diseñar detecciones basadas en comportamiento y priorizar controles.
- https://attack.mitre.org/



Extracto de TTP APT41

TTP – Tácticas, Técnicas y Procedimientos



- Las **TTP (Tácticas, Técnicas y Procedimientos)** describen **cómo actúan los atacantes**: qué buscan, cómo lo hacen y de qué forma lo ejecutan.
- Su relevancia radica en que permiten **entender el comportamiento del adversario** y **mejorar la detección, respuesta y defensa proactiva** frente a ataques reales.
- MITRE ATT&CKProporciona una solida base de información de: campañas, software, controles, entre otros.

Amenazas

Panorama de Amenazas 2024 - ENISA

Amenazas Emergentes 2030 - ENISA

- **Amenaza:** es cualquier evento, acción o situación que **puede causar daño o afectar** a una organización, sistema o persona.

Vulnerabilidades – ISO 27005

Category	No.	Examples of vulnerabilities
Hardware	VH01	Insufficient maintenance/faulty installation of storage media
	VH02	Insufficient periodic replacement schemes for equipment
	VH03	Susceptibility to humidity, dust, soiling
	VH04	Sensitivity to electromagnetic radiation
	VH05	Insufficient configuration change control
	VH06	Susceptibility to voltage variations
	VH07	Susceptibility to temperature variations
	VH08	Unprotected storage
	VH09	Lack of care at disposal
	VH10	Uncontrolled copying
Software	VS01	No or insufficient software testing
	VS02	Well-known flaws in the software
	VS03	No 'logout' when leaving the workstation
	VS04	Disposal or reuse of storage media without proper erasure
	VS05	Insufficient configuration of logs for audit trail's purposes
	VS06	Wrong allocation of access rights
	VS07	Widely-distributed software
	VS08	Applying application programs to the wrong data in terms of time
	VS09	Complicated user interface
	VS10	Insufficient or lack of documentation
	VS11	Incorrect parameter set up
	VS12	Incorrect dates
	VS13	Insufficient identification and authentication mechanisms (e.g. for user authentication)
	VS14	Unprotected password tables
	VS15	Poor password management
	VS16	Unnecessary services enabled
	VS17	Immature or new software
	VS18	Unclear or incomplete specifications for developers
	VS19	Ineffective change control
	VS20	Uncontrolled downloading and use of software
	VS21	Lack of or incomplete back-up copies
	VS22	Failure to produce management reports
Network	VN01	Insufficient mechanisms for the proof of sending or receiving a message
	VN02	Unprotected communication lines
	VN03	Unprotected sensitive traffic
	VN04	Poor joint cabling
	VN05	Single point of failure
	VN06	Ineffective or lack of mechanisms for identification and authentication of sender and receiver
	VN07	Insecure network architecture
	VN08	Transfer of passwords in clear
	VN09	Inadequate network management (resilience of routing)
	VN10	Unprotected public network connections

Category	No.	Examples of vulnerabilities
Personnel	VP01	Absence of personnel
	VP02	Inadequate recruitment procedures
	VP03	Insufficient security training
	VP04	Incorrect use of software and hardware
	VP05	Poor security awareness
	VP06	Insufficient or lack of monitoring mechanisms
	VP07	Unsupervised work by outside or cleaning staff
	VP08	Ineffective or lack of policies for the correct use of telecommunications media and messaging
Site	VS01	Inadequate or careless use of physical access control to buildings and rooms
	VS02	Location in an area susceptible to flood
	VS03	Unstable power grid
	VS04	Insufficient physical protection of the building, doors and windows
Organization	VO01	Formal procedure for user registration and de-registration not developed, or its implementation is ineffective
	VO02	Formal process for access right review (supervision) not developed, or its implementation is ineffective
	VO03	Insufficient provisions (concerning security) in contracts with customers and/or third parties
	VO04	Procedure of monitoring of information processing facilities not developed, or its implementation is ineffective
	VO05	Audits (supervision) are not conducted on regular base
	VO06	Procedures of risk identification and assessment not developed, or its implementation is ineffective
	VO07	Insufficient or lack of fault reports recorded in administrator and operator logs
	VO08	Inadequate service maintenance response
	VO09	Insufficient or lack of Service Level Agreement
	VO10	Change control procedure not developed, or its implementation is ineffective
	VO11	Formal procedure for ISMS documentation control not developed, or its implementation is ineffective
	VO12	Formal procedure for ISMS record supervision not developed, or its implementation is ineffective
	VO13	Formal process for authorization of public available information not developed, or its implementation is ineffective
	VO14	Improper allocation of information security responsibilities
	VO15	Continuity plans do not exist, or are incomplete, or are outdated
	VO16	E-mail usage policy not developed, or its implementation is ineffective
	VO17	Procedures for introducing software into operational systems not developed, or their implementation is ineffective
	VO18	Procedures for classified information handling not developed, or their implementation is ineffective
	VO19	Information security responsibilities are not present in job descriptions
	VO20	Insufficient or lack of provisions (concerning information security) in contracts with employees
	VO21	Disciplinary process in case of information security incident not defined, or not functioning properly
	VO22	Formal policy on mobile computer usage not developed, or their implementation is ineffective

Vulnerabilidad: es una **debilidad o falla** que puede ser **aprovechada por una amenaza** para causar ese daño.

Vulnerabilidades de Software

Impactos en el Negocio

Nivel de Impacto	Financieros	Operacionales	Tecnológicos	Ciberseguridad	Reputación	Legales / Regulatorios	Privacidad
🟥 5 – Catastrófico	Pérdida > 5% de ingresos anuales o quiebra.	Interrupción > 5 días o pérdida total de capacidad operativa.	Falla masiva o pérdida completa de infraestructura crítica.	Exfiltración masiva de datos, ransomware total o crisis de disponibilidad.	Crisis reputacional internacional, pérdida de clientes clave o confianza pública.	Sanción severa, suspensión de licencia, demandas o acción penal.	Exposición masiva de datos personales o sensibles con sanción y pérdida de confianza institucional.
🟧 4 – Alto	Pérdida entre 3% y 5% de ingresos.	Interrupción 3–5 días con impacto significativo en clientes o servicios.	Caída prolongada de sistemas esenciales.	Brecha de datos sensibles o cifrado generalizado.	Noticia nacional, pérdida notable de reputación o impacto en stakeholders.	Multa alta > 1.000 UTM o litigio relevante.	Filtración parcial de datos sensibles o denuncias ante autoridad.
🟨 3 – Moderado	Pérdida entre 1% y 3% de ingresos.	Interrupción 1–2 días o retrasos relevantes.	Falla en sistema crítico con degradación operativa.	Compromiso parcial o intento exitoso limitado de intrusión.	Noticia local o daño reputacional moderado.	Multa menor o observación formal.	Exposición limitada de datos no sensibles.
🟦 2 – Bajo	Pérdida entre 0,5% y 1% de ingresos.	Interrupción < 8 h o reprocesos menores.	Falla parcial en sistemas no críticos.	Intento de ataque detectado y contenido.	Reclamo aislado o mención negativa leve.	Observación regulatoria sin sanción.	Fuga potencial o acceso indebido contenido sin exposición pública.
🟩 1 – Muy Bajo	Pérdida < 0,5% de ingresos.	Interrupción menor < 2 h sin afectación crítica.	Falla menor o degradación temporal sin impacto al cliente.	Evento interno detectado sin afectación ni compromiso.	Sin impacto externo ni visibilidad pública.	Incumplimiento administrativo interno leve.	Sin afectación ni riesgo a la información personal.

Impactos en el Negocio visión más aplicada

Nivel de Impacto	Salud (atenciones / mortalidad)	Gastronomía (pérdida de alimentos / clientes)	Educación (clases / horas perdidas)	Telecomunicaciones (servicio y usuarios)	Minería (operacional / financiero)	Pensiones (servicio y confianza)
🟥 5 – Catastrófico	Interrupción total de servicios críticos (>60% de atenciones suspendidas) o ≥3 fallecidos.	Pérdida total de alimentos o cierre prolongado con >70% de caída en comensales.	Suspensión total de clases >5 días o pérdida del trimestre académico.	Caída nacional o >50% de usuarios sin servicio ≥6 h; interrupción de comunicaciones de emergencia.	Paralización total de faenas o pérdida ≥5% producción (>US$25M).	Interrupción total de pagos ≥12 h o inaccesibilidad a fondos; daño reputacional severo y afectación masiva a adultos mayores.
🟧 4 – Alto	Pérdida del 40–60% de atenciones o pacientes en riesgo sin fallecidos.	Pérdida del 40–70% de alimentos o cierre temporal (>3 días) con daño reputacional.	Suspensión de clases 2–5 días o pérdida >10% de horas pedagógicas.	Corte regional o degradación >30% de usuarios ≥3 h; afectación de servicios críticos (banca, salud, seguridad).	Interrupción operativa ≥1 día o pérdida 2–5% de producción (>US$10M).	**Retraso o interrupción en pagos ≥2 horas**, errores masivos en montos, accesos o acreditaciones; impacto directo en beneficiarios vulnerables.
🟨 3 – Moderado	Reducción del 20–40% de atenciones o retrasos con pacientes críticos.	Pérdida del 20–40% de alimentos o caída del 30–50% en ventas.	Suspensión parcial de clases (1 día completo) o pérdida 5–10% de horas pedagógicas.	Degradación parcial (10–30% usuarios) ≥1 h; interrupción localizada con reclamos.	Interrupción de 6–12 h o reducción parcial de operaciones (<2% producción).	**Retrasos entre 1 y 2 horas** en pagos o acreditaciones; errores aislados pero con reclamos públicos.
🟦 2 – Bajo	Reducción <20% de atenciones, sin daño clínico.	Pérdida <20% de alimentos o retraso leve.	Retraso menor o suspensión puntual de clases (<4 h).	Falla breve <1 h, impacto <10% usuarios o microcortes locales.	Interrupción <6 h, costos menores o ajuste operativo limitado.	**Retrasos menores <1 hora**, fallas puntuales o errores corregidos sin impacto al beneficiario.
🟩 1 – Muy Bajo	Afectación puntual sin impacto clínico.	Pérdida mínima sin afectar servicio.	Afectación leve sin pérdida de clases.	Degradación mínima sin reclamos.	Ajustes operativos menores, sin pérdida productiva.	Atención normal y pagos ejecutados en tiempo.

Gestión de Incidentes de Ciberseguridad

Proceso de Gestión de Incidentes

- Detectar y responder rápidamente a incidentes de seguridad para minimizar impacto.
- Coordinar equipos técnicos, negocio, proveedores y autoridades cuando corresponde.
- Preservar evidencia para investigación y cumplimiento regulatorio.
- Restablecer continuidad de servicios afectados de manera controlada.
- Comunicar oportunamente a stakeholders clave (internos/externos).
- Generar lecciones aprendidas que alimenten mejora del SGSI y controles preventivos.

Etapa	Descripción	Resultado esperado	Evidencias verificables
1. Preparación	Definir roles, contactos, herramientas, playbooks y capacidades.	Plan de Respuesta a Incidentes (PRI) vigente.	Procedimiento IR, contactos, plantillas, entrenamiento, simulaciones.
2. Detección y Análisis	Identificación de anomalías o señales de compromiso.	Ticket de incidente con clasificación inicial.	Alertas SIEM/EDR, análisis de logs, correlación MITRE ATT&CK.
3. Contención Inicial	Limitar el alcance y evitar propagación o daño mayor.	Incidente aislado y contenido.	Evidencia de bloqueo, desactivación, microsegmentación, snapshots.
4. Erradicación y Remediación	Eliminar la causa raíz y restaurar configuraciones seguras.	Riesgo eliminado o mitigado.	Reportes de remediación, parches aplicados, reposición de configuraciones.
5. Recuperación	Restablecer servicio en forma **controlada y validada**.	Servicio restablecido sin reinfección.	Bitácoras de recuperación, validación post-restauración, pruebas de integridad.
6. Lecciones Aprendidas y Cierre	Mejorar procesos y controles basados en el incidente.	Informe final + acciones de mejora.	Analisis forense, RCA (Root Cause Analysis), actualización de playbooks y controles.

Guía de Clasificación de Incidentes de Enisa

CRÍTICO	Otros	APT
		Ciberterrorismo
		Daños informáticos PIC
MUY ALTO	Código dañino	Distribución de malware
		Configuración de malware
	Intento de intrusión	Ataque desconocido
	Intrusión	Robo
	Disponibilidad	Sabotaje
		Interrupciones
ALTO	Contenido abusivo	Pornografía infantil, contenido sexual o violento inadecuado
	Código dañino	Sistema infectado
		Servidor C&C (Mando y Control)
	Intento de intrusión	Malware dominio DGA
		Compromiso de aplicaciones
	Disponibilidad	DoS (Denegación de servicio)
		DDoS (Denegación distribuida de servicio)
	Compromiso de la información	Acceso no autorizado a información
		Modificación no autorizada de información

		Pérdida de datos
	Fraude	Phishing
MEDIO	Contenido abusivo	Discurso de odio
	Obtención de información	Ingeniería social
		Explotación de vulnerabilidades conocidas
	Intento de intrusión	Intento de acceso con vulneración de credenciales
	Intrusión	Compromiso de cuentas con privilegios
	Fraude	Uso no autorizado de recursos
		Derechos de autor
		Suplantación
	Vulnerable	Criptografía débil
		Amplificador DDoS
		Servicios con acceso potencial no deseado
		Revelación de información
		Sistema vulnerable
BAJO	Contenido abusivo	Spam
	Obtención de información	Escaneo de redes (scanning)
		Análisis de paquetes (sniffing)
	Intrusión	Compromiso de cuenta sin privilegios
	Otros	Otros

Definición Importante

Gestión de Incidente de Seguridad de la Información

- "Ejercicio de un enfoque consistente y efectivo para el manejo de incidentes de seguridad de la información"

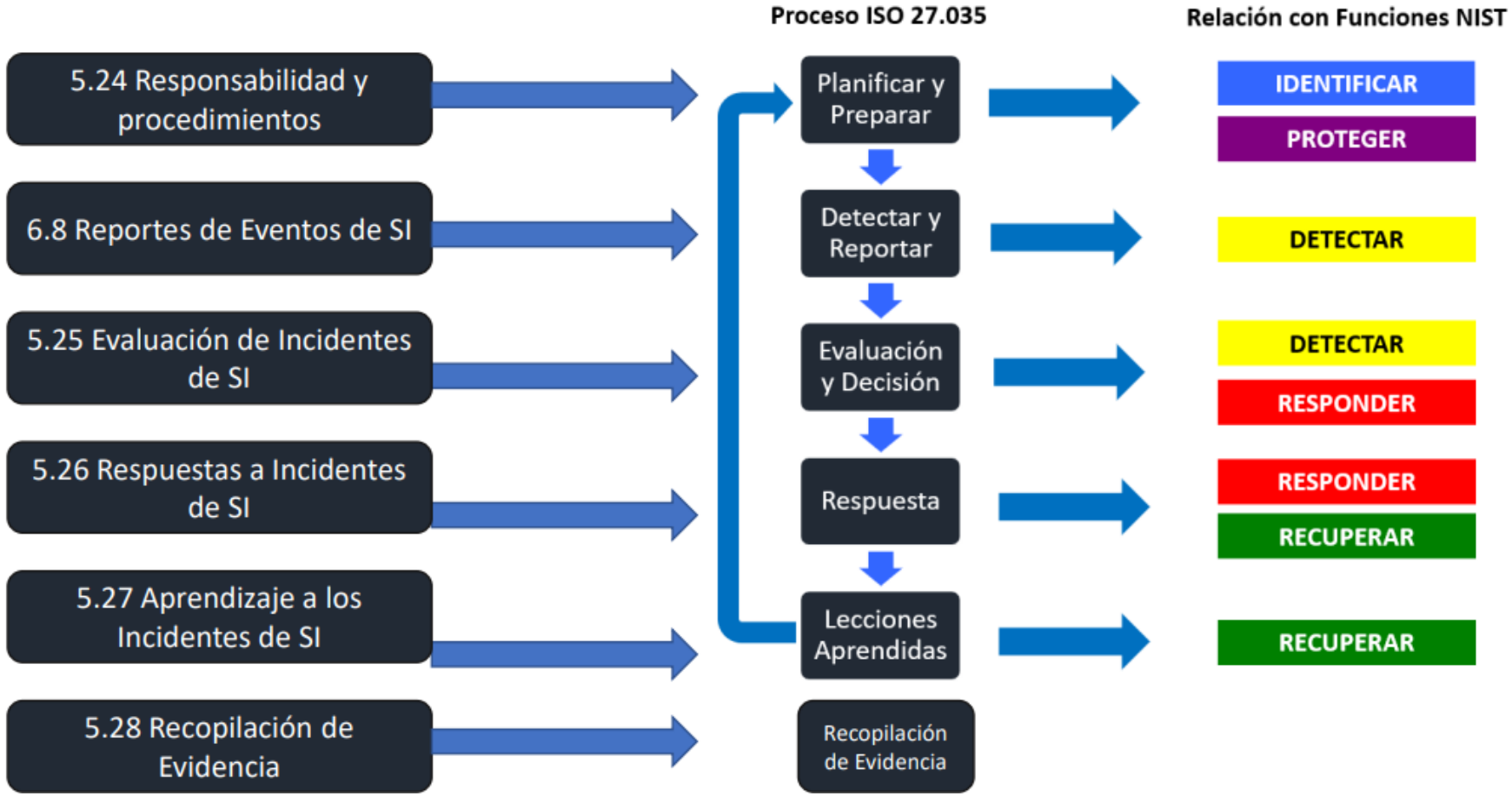
- "Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información."

Definición a veces algo conflictivo

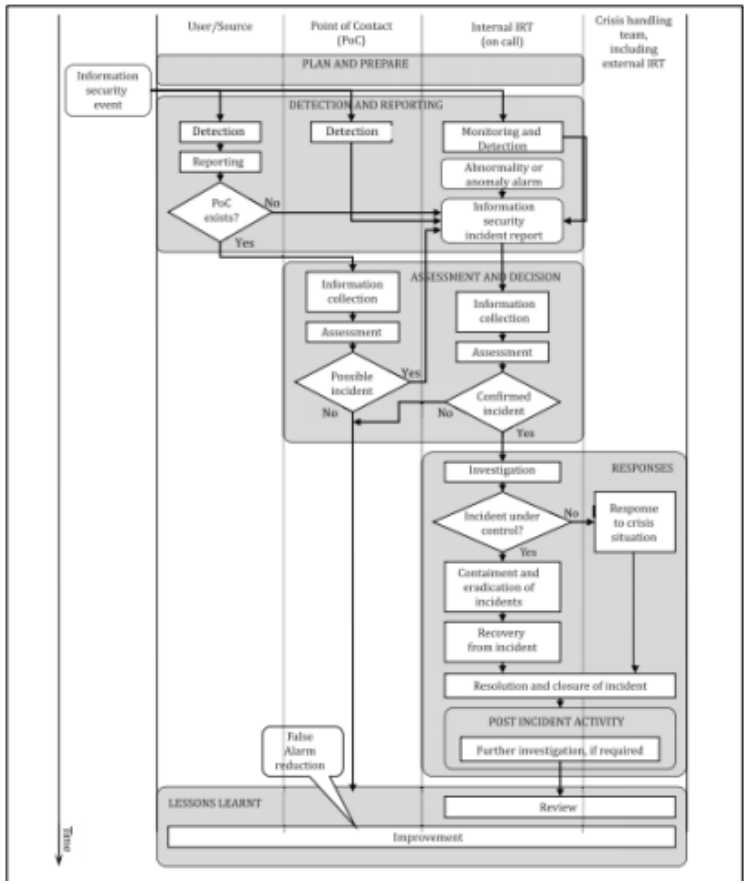
- **Evento de Seguridad de la Información**
  - "Ocurrencia que indica una posible violación de la seguridad de la información o falla de los controles"

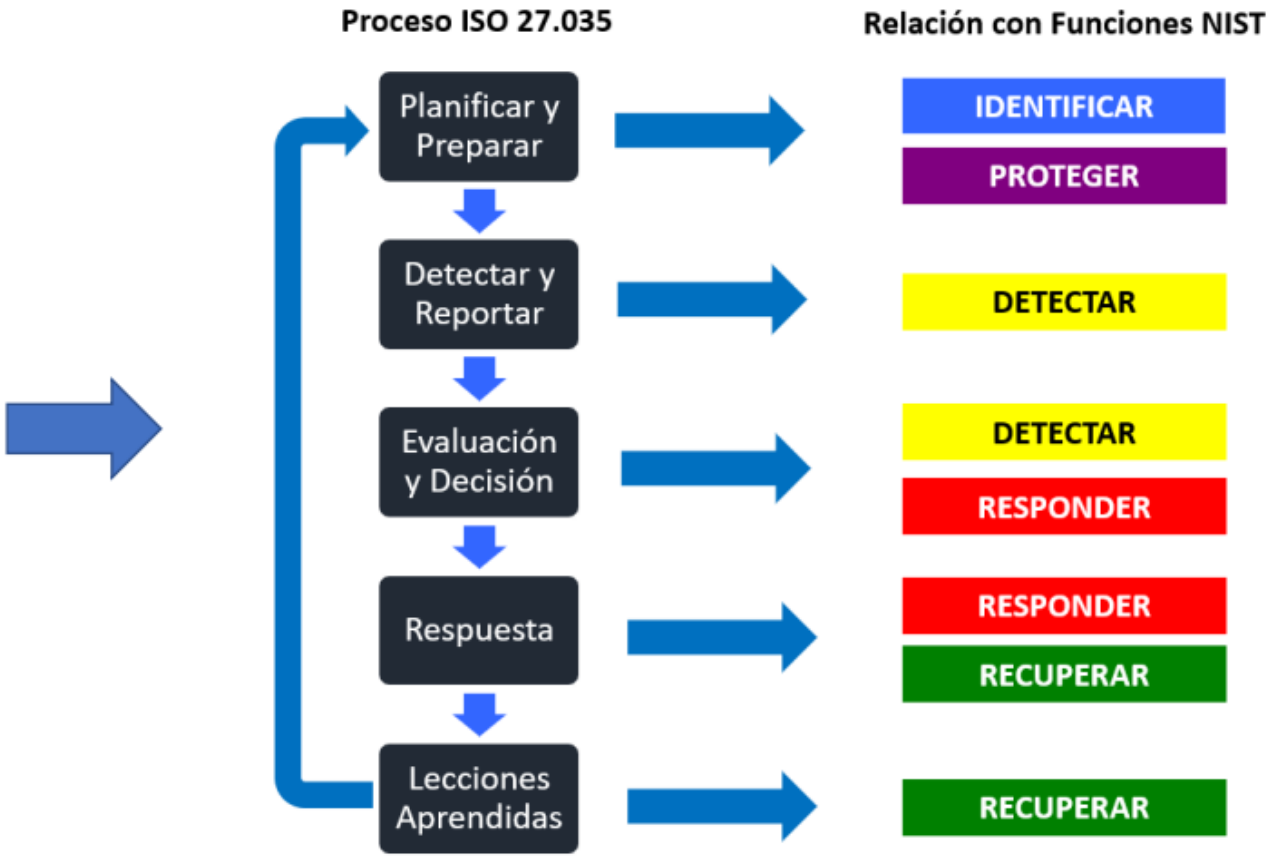
- **Incidente de Seguridad de la Información**
  - "Uno o varios eventos de seguridad de la información relacionados e identificados que pueden dañar los activos de la organización y/o comprometer sus operaciones"

El proceso


Proceso ISO 27.035
Relación con Funciones NIST
5.24 Responsabilidad y procedimientos
6.8 Reportes de Eventos de SI
5.25 Evaluación de Incidentes de SI
5.26 Respuestas a Incidentes de SI
5.27 Aprendizaje a los Incidentes de SI
5.28 Recopilación de Evidencia
Planificar y Preparar
Detectar y Reportar
Evaluación y Decisión
Respuesta
Lecciones Aprendidas
Recopilación de Evidencia
IDENTIFICAR
PROTEGER
DETECTAR
DETECTAR
RESPONDER
RESPONDER
RECUPERAR
RECUPERAR

El proceso


User/Source
Point of Contact (PoC)
Internal IRT (on call)
Crisis handling team, including external IRT
PLAN AND PREPARE
Information security event
DETECTION AND REPORTING
Detection
Reporting
Detection
Monitoring and Detection
Abnormality or anomaly alarm
PoC exists?
No
Yes
Information security incident report
ASSESSMENT AND DECISION
Information collection
Assessment
Possible incident
Yes
No
Information collection
Assessment
Confirmed incident
No
Yes
RESPONSES
Investigation
Incident under control?
No
Yes
Response to crisis situation
Containment and eradication of incidents
Recovery from incident
Resolution and closure of incident
POST INCIDENT ACTIVITY
Further investigation, if required
False Alarm reduction
LESSONS LEARNT
Review
Improvement
Time


Proceso ISO 27.035
Relación con Funciones NIST
Planificar y Preparar
Detectar y Reportar
Evaluación y Decisión
Respuesta
Lecciones Aprendidas
IDENTIFICAR
PROTEGER
DETECTAR
DETECTAR
RESPONDER
RESPONDER
RECUPERAR
RECUPERAR

Planificación

- Alineado a definiciones claves de gobernanza y gestión de incidentes
  - Compromiso de la dirección
  - Definición de estructuras organizacionales, roles y responsabilidades
  - Políticas , procedimientos, metodologías,….
  - Concientización y capacitación
  - Relaciones con terceros
  - Las herramientas requeridas

PLAN AND PREPARE

- information security incident management policy, and commitment of top management
- information security policies, including those related to risk management, updated at both corporate level and system, service, and network levels
- information security incident management plan
- IRT establishment
- relationships and connections with internal and external organizations
- technical and other support (including organizational and operational support)
- information security incident management awareness briefings and training
- information security incident management plan testing

Metodología

Formato y tipo de reporte

B.4 Example forms

B.4.1 Example form for information security event report

INFORMATION SECURITY EVENT REPORT			Page 1 of 1
1. Date of event		3. Related event and/or incident identity numbers *(if applicable)*	
2. Event number[2]			
4. REPORTING PERSON DETAILS			
4.1 Name		4.2 Address	
4.3 Organization		4.4 Department	
4.5 Telephone		4.6 E-mail	
5. INFORMATION SECURITY EVENT DESCRIPTION			
5.1 Description of the event: What occurred How occurred Why occurred Initial views on components/assets affected Adverse business impacts Any vulnerabilities identified			
6. INFORMATION SECURITY EVENT DETAILS			
6.1 Date and time the event occurred			
6.2 Date and time the event was discovered			

INFORMATION SECURITY INCIDENT REPORT	Page 2 of 6
8. INFORMATION SECURITY INCIDENT CATEGORY	

(Tick one, then complete related section below.)
8.1 Actual *(incident has occurred)* ☐
8.2 Suspected *(incident thought to have occurred but not confirmed)* ☐

(One of) **8.3 Natural disaster** ☐ *(indicate threat types involved)*

☐ Earthquake ☐ Volcano ☐ Flood ☐ Violent wind
☐ Lightning ☐ Tsunami ☐ Collapse ☐ Other

Specify:

(One of) **8.4 Social unrest** ☐ *(indicate threat types involved)*

☐ Protest ☐ Terrorist assault ☐ War ☐ Other

Specify:

(One of) **8.5 Physical damage** ☐ *(indicate threat types involved)*

☐ Fire ☐ Water ☐ Electrostatic
☐ Abominable environment (such as pollution, dust, corrosion, freezing)
☐ Destruction of equipment ☐ Destruction of media ☐ Theft of equipment
☐ Theft of media ☐ Loss of equipment ☐ Loss of media
☐ Tampering with equipment ☐ Tampering with media ☐ Other

Specify:

(One of) **8.6 Infrastructure failure** ☐ *(indicate threat types involved)*

☐ Power-supply failure ☐ Networking failure ☐ Air-conditioning failure
☐ Water-supply failure ☐ Other

Specify:

(One of) **8.7 Radiation disturbance** ☐ *(indicate threat types involved)*

☐ electromagnetic radiation ☐ lectromagnetic pulse ☐ Electronic jamming
☐ Voltage fluctuation ☐ Thermal radiation ☐ Other

Herramientas – Ejemplo McAfee

CSF Function	Category	Cyber Solution Mapping
Identify (ID)	• Asset Management • Business Environment • Governance • Risk Assessment • Risk Management Strategy	• Application Performance Management • Network Performance Management • Network Infrastructure Security Management • Governance, Risk, and Compliance (GRC) Tools • Security Information and Event Management (SIEM)
Protect (PR)	• Access Control • Awareness and Training • Data Security • Information Protection Processes and Procedures • Maintenance • Protective Technology	• Full Disk Encryption • Removable Media and File and Folder Encryption • Next-Generation Firewall • Intrusion Prevention System (IPS)/ Intrusion Detection System (IDS) • Network Access Control (NAC) • Web and Email Gateways/Forward Proxy • Application Delivery Controller (ADC)/Reverse Proxy • Web Application Firewall (WAF) • Data Loss Prevention (DLP) • Security Information and Event Management (SIEM) • Privileged User Access Control • Role-Based Data Encryption • Unstructured Data Protection

CSF Function	Category	Cyber Solution Mapping
Detect (DE)	• Anomalies and Events • Security Continuous Monitoring • Detection Processes	• NGFW • IPS/IDS • NAC • Web and Email Gateways/Forward Proxy • ADC/Reverse Proxy/WAF • DLP • Endpoint Threat Detection • Network Behavior Analysis • Honeypots • Sandbox Analysis • SIEM
Respond (RS)	• Response Planning • Communications • Analysis • Mitigation • Improvements	• Endpoint Threat Detection and Response (ETDR) • Network Behavior Analysis • GRC Tools • Local/Global Threat Feed Tools • Security Operations Center (SOC) Automation
Recover (RC)	• Recovery Planning • Improvements • Communications	• Data replication and backup • DR COOP Sites

5.3 .- Detección y Reporte

- Establecimiento del proceso, el cual considera:
  - El desarrollo de la concientización, considerando factores externos
  - Los sistemas de monitoreo
  - Detección de actividad anómala, sospechosa y/o maliciosa
  - Recolección de eventos de seguridad de terceras partes relevantes
  - Reporte de eventos de seguridad de la información

DETECTION AND REPORTING

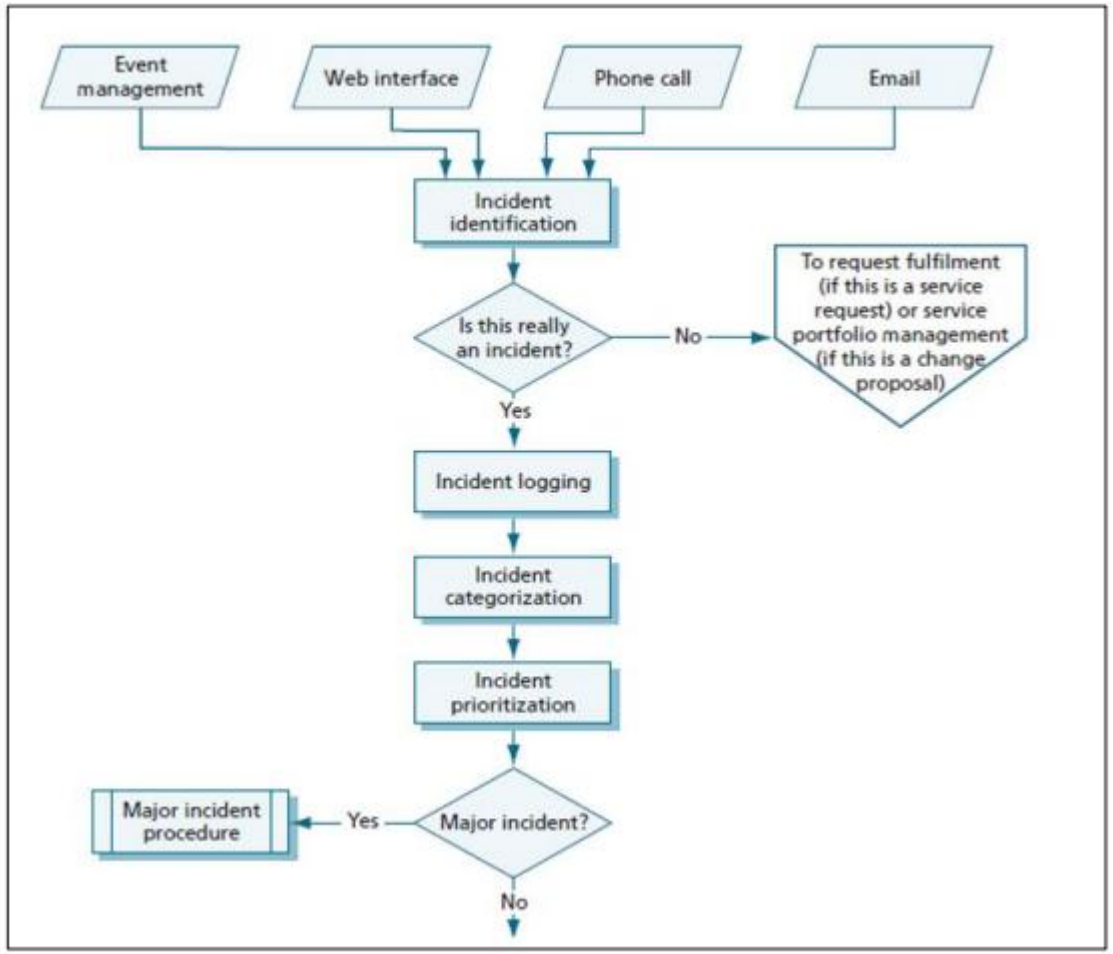
- collecting situational awareness information from local environment and external data sources and news feeds
- monitoring of constituency systems and networks
- detection and alerting of anomalous, suspicious or malicious activities
- collection of information security event reports from constituents, vendors, other IRTs or security organizations and automated sensors
- reporting information security events

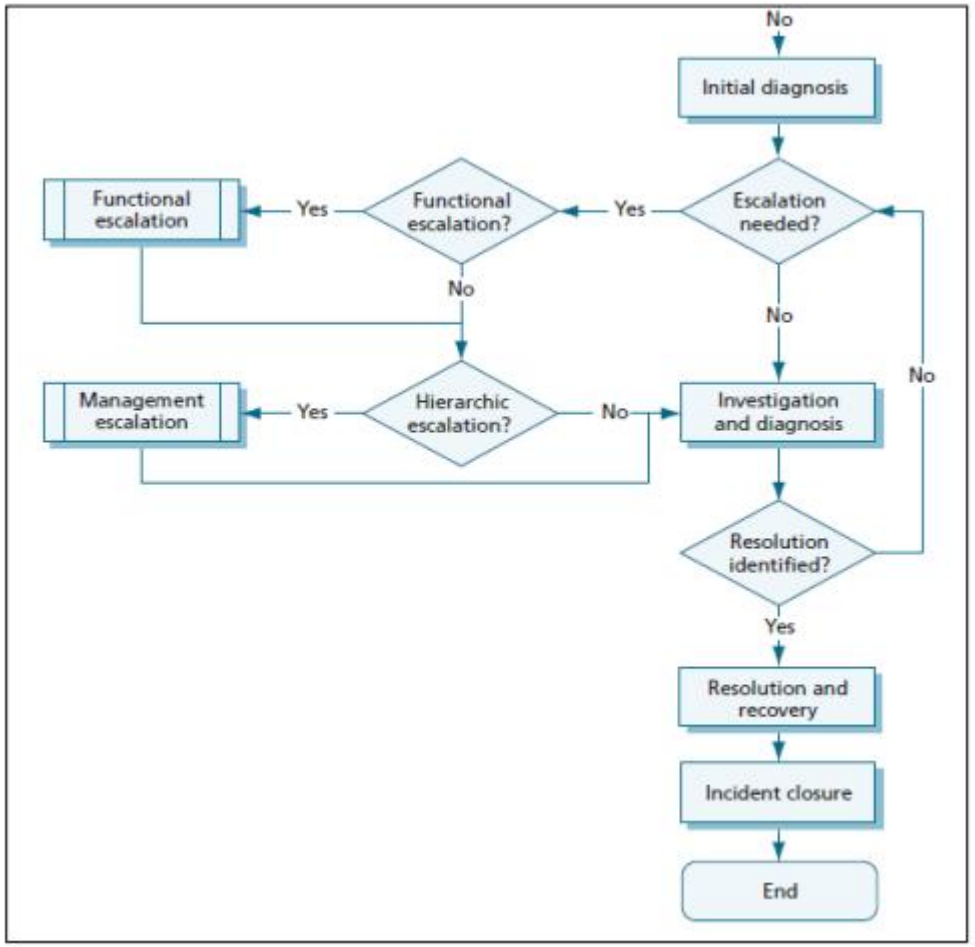
6.8 Reporte de eventos de seguridad de la información

- Potenciales situaciones cuando reportar

Inefectividad de un control	Brecha de expectativas de CID	Errores Humanos	Incumplimiento
Brechas de Seguridad Física	Cambios no formalizados	Malfuncionamiento de Sw/Hw	Violación de Acceso
	Vulnerabilidades	Sospecha de infección con malware	

Ejemplo de ITIL





5.4.- Evaluación y decisión

- Básicamente el proceso de evaluación de incidentes.
- Debe considerar los mecanismo de detección y reporte.
- Acá se determina si el evento es un incidente o no, luego:
  - Debe establecerse el proceso de evaluación
  - Debe definirse un proceso de clasificación de incidentes
  - Establecer tiempos de respuestas y niveles de escalamiento

DETECTION AND REPORTING

- collecting situational awareness information from local environment and external data sources and news feeds
- monitoring of constituency systems and networks
- detection and alerting of anomalous, suspicious or malicious activities
- collection of information security event reports fromconstituents, vendors, other IRTs or security organizations and automated sensors
- reporting information security events

5.5.- Respuesta

- El etapa en la cual se gestiona el incidente para su resolución.
  - Se emplean los diversos planes de acción (playbooks) para su erradicación
  - Se activan planes de continuidad y DRP en caso de ser necesario
  - Se integran con procesos de comunicación
  - En caso de ser requerido se realiza investigación adicional (forense)
  - El resultado de la etapa es el cierre del incidente.

RESPONSES

- determination of whether information security incidents are under control by investigation
- containment and eradication of information security incidents
- recovery from information security incidents
- resolution and closure of information security incidents

POST INCIDENT ACTIVITY

- further investigation, if required

5.6.- Lecciones Aprendidas

Actor / Artefacto	Acciones	Deficiencia en Control
	El atacante envía un correo a cuentas válidas del dominio	
	El correo electrónico ingresa al buzón del usuario	 **Antispam:** Falla al validar el origen, la reputación y el contenido
	El usuario da clic sobre el archivo malicioso Ej: citacion.docx	 **Conciencia en Seguridad:** El usuario falla al no seguir las recomendaciones referentes a ingeniería social.
	El archivo se ejecuta, descarga archivos binarios, establece comunicación contra los servidores maliciosos y negocia el cifrado	 **Filtrado Web:** Falla al permitir conexiones contra servidores no autorizados
	Se produce el cifrado de datos, se eliminan los Shadow Copies y se presentan las notas del rescate de la información. La amenaza se propaga a través del protocolo SMBv1	 **Gestión de Parches:** Se evidencia falta de parches de seguridad y debilidad en el diseño de la red.
	El usuario no puede recuperar la información, teniendo en cuenta que la única forma de recuperación es un backup reciente.	 **Backups:** No se cuenta con políticas y procedimientos de backup periódicos.
		WannaCry | ShieldNow Playbook

- Tomar acciones
- ¿Qué fallo?
- ¿Que mejora?
- ¿Cómo mejorar?
- ¿Mejorar?

- Proceso continuo a lo largo del ciclo

- Hacer Playbook sobre incidentes.

Fuente: https://shieldnow.co/2017/05/13/wannacry-lecciones-aprendidas/

Consideraciones Ley

- Decreto Supremo 295 (2024) establece contenido y tiempos en los cuales deben enviarse los reportes de incidentes.

- Resolución 7 Exenta (2025) define la taxonomía de incidentes a reportar, es decir, que tipo de incidentes son los que deben ser reportados.

- Ley Marco (Articulo N°9) establece la obligación de reportar al CSIRT Nacional los ciberataques e incidentes de ciberseguridad que puedan tener efectos significativos en los términos del artículo 27° de la ley, tan pronto les sea posible y conforme al esquema establecido en dicho artículo.

- Debe poseerse los procedimientos y capacidades necesarias para dar respuesta a la Ley, sobre todo en los tiempos que esta define.

- Quienes deben reportar?
  - PSE y OIV

Consideraciones bases

Enviar una alerta temprana sobre la ocurrencia del evento en máximo 3 horas.

Actualización de la información con: evaluación inicial, gravedad, impacto e IoC, en 72 horas.

Informe final, máximo en 15 días corridos.

CSIRT Nacional podrá pedir actualizaciones.

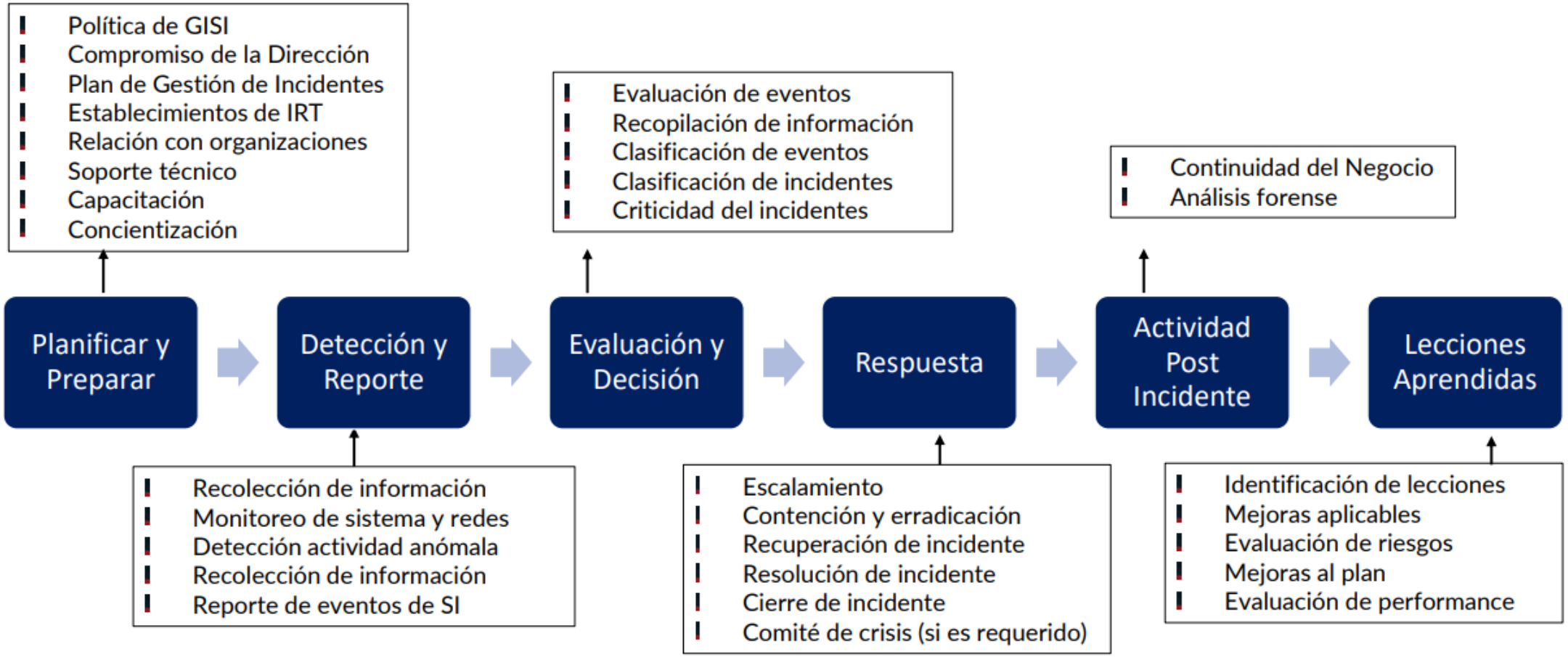
OIV deberán informar al CSIRT Nacional plan de acción.

Los contratos no podrán contener ninguna cláusula que restringa o dificulte la comunicación de información sobre amenazas por parte del prestador de servicios.

La Agencia dictará instrucciones para la realización y recepción de los reportes.

Charla ANCI Ley Marco de Ciberseguridad 2025 marzo

Proceso de Gestión de Incidentes – Desde ISO 27035



5.24 Planificación y preparación (ISO 27002)

Roles y Responsabilidades

- Método común de reporte
- Proceso de Gestión de Incidentes
- Proceso de Respuesta a Incidentes
- Competencia Profesional
- Identificar training requerido

Procedimientos

- Evaluación de Eventos
- Detección y análisis de eventos e incidentes
- Escalamiento y Respuesta
- Manejo de Evidencia
- Análisis de la causa
- Lecciones Aprendidas

Procedimiento de Reporte

- Acciones frente a un evento
- Uso de Formularios
- Proceso de retroalimentación
- Creación de informes de incidentes

Resumen de Controles de Gestión de Incidentes – ISO 27002

Control	Nombre del Control	Tipo de Controles	Propiedades de seguridad de la información	Conceptos de ciberseguridad	Capacidades operacionales	Dominios de seguridad
5,24	Responsabilidades y procedimientos	#Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Responder #Recuperar	#Información_seguridad_gestión_de_eventos	#Defensa
5,25	Evaluación y decisión sobre los eventos de seguridad de información	#Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar #Responder	#Información_seguridad_gestión_de_eventos	#Defensa
5,26	Respuesta a incidentes de seguridad de la información	#Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Responder #Recuperar	#Información_seguridad_gestión_de_eventos	#Defensa
5,27	Aprendizaje de los incidentes de seguridad de la información	#Preventivo	#Confidencialidad #Integridad #Disponibilidad	#Proteger #Identificar	#Información_seguridad_gestión_de_eventos	#Defensa
5,28	Recopilación de evidencias	#Detectivo #Correctivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar #Responder	#Información_seguridad_gestión_de_eventos	#Defensa
6,80	Reporte de eventos de seguridad de la información	#Detectivo	#Confidencialidad #Integridad #Disponibilidad	#Detectar	#Información_seguridad_gestión_de_eventos	#Defensa

Resumen de Controles de Gestión de Incidentes – ISO 27002

Marco	Sección / Control	Qué exige
ISO 27001:2022	A.5.25–A.5.28	Preparación, detección, respuesta, mejoras.
ISO 27002:2022	**8.16, 8.18, 8.19, 8.20**	Gestión de logs, monitoreo, clasificación y respuesta.
ISO 27035 (1/2/3)	**Norma específica para gestión de incidentes**	Proceso completo y guías operativas.
NIST SP 800-61r2	*Computer Security Incident Handling Guide*	Framework IR más usado globalmente.
CIS Controls v8.1	Control 17 – IR & Testing	Equipos, playbooks, entrenamiento y simulaciones.
MITRE ATT&CK	Base para análisis de TTPs	Entender el comportamiento del adversario.

Ley	Exigencia
Ley Marco de Ciberseguridad	*Notificación de incidentes significativos a CSIRT/ANCI*
Ley 21.719 (Protección de Datos)	Notificar **brechas de datos personales** según severidad

Gestión de Continuidad del Negocio

Proceso de Gestión de Continuidad del Negocio

- Asegurar la recuperación y continuidad de los servicios críticos frente a incidentes disruptivos.
- Proteger la confidencialidad, integridad y disponibilidad de la información durante contingencias.
- Minimizar impactos financieros, reputacionales, operacionales y regulatorios.
- Establecer planes, roles y procedimientos claros para responder y recuperar en tiempos aceptables.
- Alinear la continuidad con las prioridades estratégicas del negocio (procesos críticos).
- Garantizar la resiliencia, no solo la recuperación: capacidad de resistir, adaptarse y aprender.

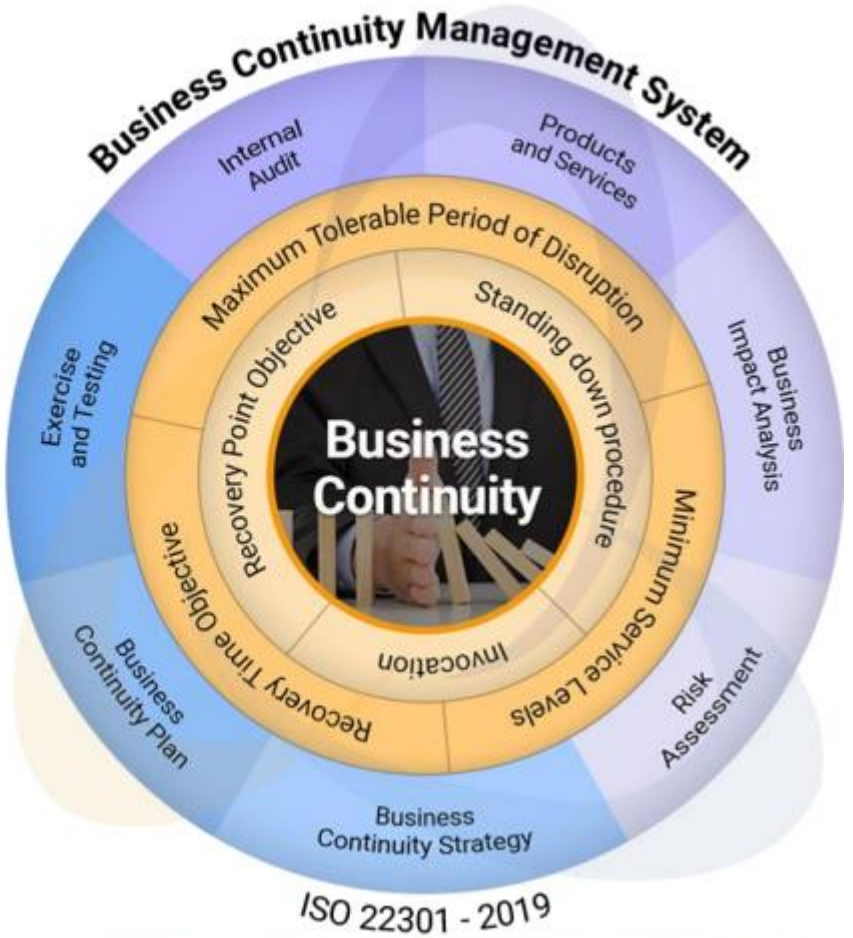
Sistema de Gestión de Continuidad del Negocio – ISO 22301

Clausula	ISO 20.000	ISO 22.301	ISO 27.001
1	Objeto y ámbito de aplicación.		
2	Referencias normativas		
3	Terminología ISO 20.000-1	Terminología ISO 22.300	Terminología ISO 27.000
4	Contexto Interno y Externo, Partes Interesadas y Alcance		
5	Liderazgo, roles, responsabilidades y Política.		
6	Gestión de Servicios, Riesgos y Procesos.	Análisis de Riesgos, Análisis del Impacto en el Negocio y Planes de Continuidad	Gestión de Riesgos. controles y plan de tratamiento
7	Recursos, Competencia, Concienciación, Comunicaciones y Gestión Documental		
8	Operación del Sistema de Gestión (Implementación)		
9	Revisión de Objetivos, Auditoría Interna y Revisión de la Dirección		
10	Opciones de mejora, acciones correctivas → Mejora Continua		

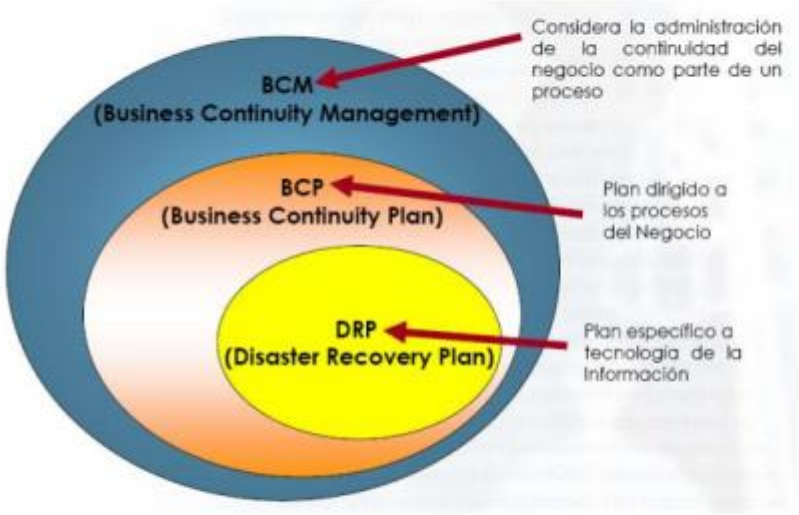
Estandarizado con cualquier Sistema de Gestión de la Familia ISO

Familia de Normas ISO 22300

- 22.300 – Vocabulario
- 22.301 – Requisitos del sistema de gestión de continuidad del negocio
- 22.313 – Directrices de Implementación
- 22.317 – Directrices para el desarrollo del BIA
- 22.320 – Directicas para la respuesta a incidentes
- 22.331 - Directrices para estrategias de continuidad
- 22.332 – Directrices para la implementación de planes de continuidad
- 22.398 – Directrices para el desarrollo de ejercicios



Evolución de la Continuidad del Negocio



DRP

Disaster Recovery Plan

- Plan orientado principalmente a recuperar todo lo relacionado con TI
- Su enfoque típicamente es:
  - Los Datos
  - Los Servicios
  - Las Aplicaciones
  - El Sistema Operativo
- Con frecuencia se ve simplemente como un SITE Alterno

BCP

Business Continuity Plan

- Plan orientado a recuperar todas las funciones críticas de la empresa y que el negocio pueda operar
- Típicamente contiene
  - DRP
  - Comités
  - Plan de Emergencia
  - Notificaciones
  - Sitios alternos de trabajo

BCM

Busines Continuity Management

- Programa continuo para todas las funciones de la empresa orientado a que
  - Cultura de BC
  - Concientización
  - Actualizacíon de todos los cambios
  - Enfoque fuerte a probar el plan para irlo mejorando

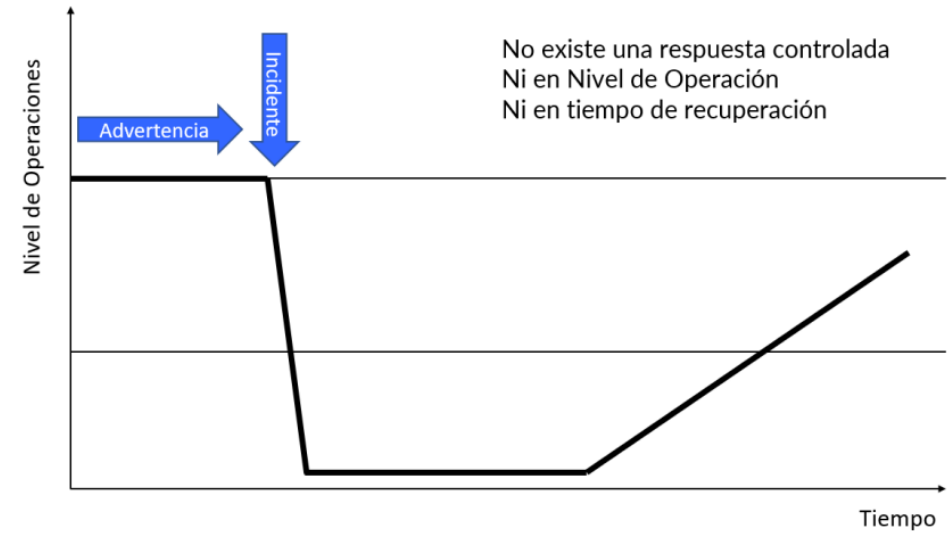
Proceso de Gestión de Continuidad del Negocio

Etapa	Descripción	Resultados esperados	Medios de Verificación / Evidencias
1. Alcance y Gobierno del Proceso	Definir los procesos, servicios, sistemas y sedes a incluir. Asignar responsables y estructura de gobernanza.	Alcance documentado y roles designados (Comité de Crisis o Continuidad).	- Documento de alcance aprobado - Nombramiento de responsables (RACI) - Actas de comité de continuidad - Organigrama funcional de crisis
2. Análisis de Impacto al Negocio (BIA)	Identificar procesos críticos, recursos necesarios y dependencias. Determinar impacto por interrupción y tolerancias.	Matriz BIA con: procesos críticos, impacto, **RTO/RPO**, MTD.	- Documento de BIA completo - Matriz de criticidad y dependencias - Validación con dueños de proceso - Evidencia de aprobación por dirección
3. Evaluación de Riesgos Disruptivos	Analizar amenazas (físicas, tecnológicas, humanas, ciber), vulnerabilidades y escenarios de falla.	Matriz de riesgo de continuidad, priorización de amenazas y escenarios.	- Matriz de riesgos (con probabilidad e impacto) - Escenarios documentados - Reporte de revisión conjunta Seguridad + Operaciones
4. Definición de Estrategias de Continuidad	Determinar cómo mantener o restaurar capacidad operacional (sitio alterno, redundancia, backup cloud, operación degradada).	Estrategia de continuidad aprobada y financiada.	- Documento de estrategia de continuidad - Costeo/ROI asociado - Acta de aprobación de la Dirección - Evidencias de contratos o capacidades disponibles
5. Desarrollo de Planes (BCP/DRP)	Redactar planes operativos por proceso y por plataforma tecnológica. Integrar roles, comunicaciones y procedimientos.	Plan de Continuidad (BCP) y Plan de Recuperación Tecnológica (DRP) versionados.	- BCP y DRP en repositorio controlado - Procedimientos paso a paso - Listado de contactos críticos - Versionado y control documental (firma / código / fecha)
6. Pruebas, Simulaciones y Ejercicios	Realizar pruebas de escritorio (tabletop), pruebas técnicas y recuperaciones programadas para validar capacidad real.	Evidencia de efectividad del plan y tiempos de recuperación reales (MTTR vs RTO).	- Informes de pruebas - Registros de resultados y desvíos - Lecciones aprendidas - Planes de acción y seguimiento
7. Revisión, Mejora y Actualización Continua	Ajustar los planes según cambios en infraestructura, personal, proveedores o auditorías. Retroalimentar el SGSI.	Planes vigentes, actualizados y alineados a la estrategia actual.	- Historial de versiones - Fechas de revisión programadas - Evidencias de actualización post incidente o post prueba - Registros de Revisión por la Dirección

Definiciones bases de Gestión de Continuidad

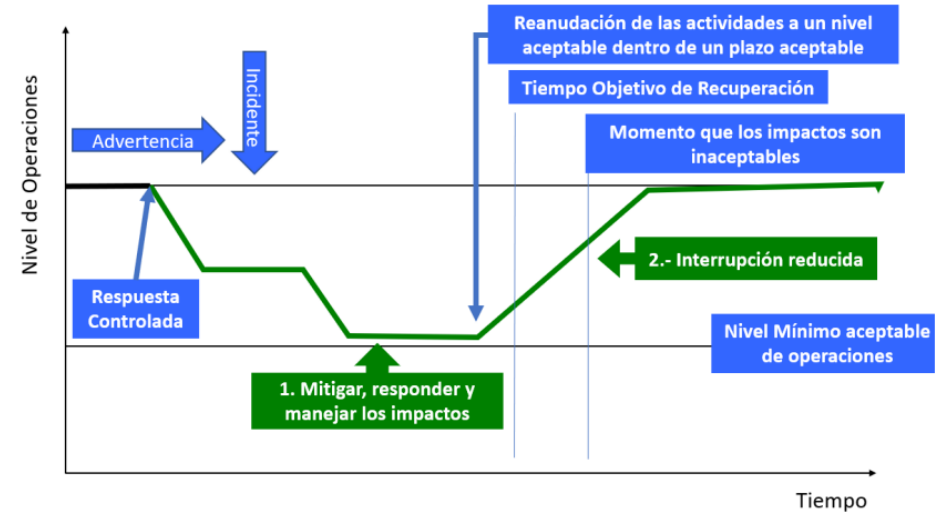
- Proceso de gestión holístico que **IDENTIFICA LAS AMENAZAS** potenciales para una organización **Y EL IMPACTO EN LAS OPERACIONES DE NEGOCIO** que esas amenazas podrían causar si se materializasen.

- Provee una estructura para **CONSTRUIR RESILIENCIA** organizacional con la **CAPACIDAD PARA LA EFECTIVA RESPUESTA** salvaguardando los intereses de las principales partes interesadas, reputación, marca y activos de valor



Fuente: ISO 22.301

Sin Continuidad



Fuente: ISO 22.301

Con Continuidad

Roles en tu gestión de crisis, continuidad frente a un ataque

Rol	Responsabilidad Clave	Competencias Específicas	Reporta a
Líder de Crisis / Comité de Crisis	Dirigir la respuesta institucional ante eventos mayores. Toma de decisiones estratégicas y comunicación oficial.	Liderazgo, gestión bajo presión, comunicación institucional, toma de decisiones.	Alta Dirección / Directorio
Coordinador de Continuidad del Negocio (BCM Manager)	Asegurar la activación del plan de continuidad, coordinar áreas críticas y evaluar tiempos de recuperación.	Conocimiento en ISO 22301, gestión de procesos críticos, análisis de impacto (BIA).	Líder de Crisis / Gerencia General
Responsable de Ciberseguridad / CISO	Dirigir la detección, contención y erradicación de incidentes cibernéticos. Garantizar integridad y disponibilidad de la información.	Experiencia en ISO 27035, MITRE ATT&CK, gestión de incidentes, SOC y CSIRT.	Comité de Crisis / Gerencia de Tecnología
Jefe de Tecnología / CIO	Mantener la operación tecnológica y ejecutar el plan de recuperación de TI (DRP).	Gestión de infraestructura, recuperación de sistemas, cloud, resiliencia técnica.	Alta Dirección / Comité de Crisis
Analista de Incidentes / CSIRT Operativo	Investigar, documentar y contener incidentes. Ejecutar acciones técnicas de respuesta.	Conocimientos en SIEM, Sysmon, forense digital, correlación de alertas, herramientas EDR.	CISO / Coordinador de Seguridad
Encargado de Comunicaciones de Crisis	Gestionar la comunicación interna y externa durante el incidente. Redactar comunicados y coordinar mensajes oficiales.	Comunicación corporativa, manejo de medios, gestión reputacional y vocería.	Líder de Crisis / Gerencia General
Asesor Legal / Compliance Officer	Evaluar obligaciones regulatorias, notificación de brechas y riesgos legales.	Conocimiento en leyes de protección de datos, ciberseguridad y continuidad.	Comité de Crisis / Gerencia General
Gerente Financiero / CFO	Analizar impactos financieros del evento y definir recursos para recuperación.	Gestión de riesgos financieros, priorización presupuestaria, continuidad contable.	Comité de Crisis / Alta Dirección
Representante de Recursos Humanos	Coordinar seguridad del personal, roles de reemplazo y bienestar durante la crisis.	Comunicación interna, liderazgo empático, gestión del cambio y continuidad operativa.	Comité de Crisis / Gerencia General
Oficial de Privacidad / DPO	Supervisar protección de datos personales y cumplimiento normativo en incidentes.	Conocimiento en Ley de Protección de Datos, GDPR, ISO 27701.	Asesor Legal / CISO
Responsable de Infraestructura y Logística	Asegurar funcionamiento físico de instalaciones alternas y recursos críticos.	Continuidad física, planes de respaldo, activación de sitios alternos, logística operativa.	Coordinador BCM / Comité de Crisis

Control 5.30 ISO 27002 - Preparación de las TIC para la continuidad del negocio

- Cambio en fondo muy relevante, con mucho más foco en la gestión de la continuidad de las TIC, antes era difuso y orientado a la continuidad de la Seguridad de la Información

Análisis del Impacto en el Negocio (BIA)

- Definir esquema de Impacto
- Determinar el impacto en el tiempo
- Priorizar en base al impacto los procesos
- Determinar los recursos necesarios
- Establecer RTO y RPO

Desarrollar Estrategias

- Basado en el análisis de riesgo y el BIA
- Puede ser una o mas alternativas
- Definir planes de continuidad

Control 5.30 ISO 27002 - Preparación de las TIC para la continuidad del negocio

- La organización debe asegurarse

Estructura Organizacional	Capacidades del personal	Planes de continuidad de TIC	Procedimientos de respuesta y recuperación
Ejercicios y pruebas	Aprobación por la Dirección	BCP alineados con el BIA	RTO de cada servicio TIC priorizados
	RPO de cada servicio TIC priorizados	Procedimientos de recuperación	

BIA (Business Impact Analysis)

- El BIA (Business Impact Analysis) o Análisis de Impacto al Negocio es el proceso que permite identificar y evaluar cómo una interrupción afecta a los procesos críticos de una organización, determinando las consecuencias operativas, financieras, legales y reputacionales.

- Su objetivo principal es priorizar qué debe recuperarse primero y en cuánto tiempo, estableciendo parámetros como el RTO (tiempo máximo de recuperación) y el RPO (pérdida máxima de datos tolerable), sirviendo como base para los planes de continuidad y recuperación.

- Resultados del BIA:
- Evaluación de criticidad de los procesos de negocio (ranking de procesos).
- Obtención de información de recursos claves relacionados con los procesos críticos de negocio.
- Determinación de períodos críticos de tiempo antes de que se experimenten pérdidas significativas (tiempo de recuperación, tiempo máximo tolerable).

Impactos en el Negocio

Nivel de Impacto	Financieros	Operacionales	Tecnológicos	Ciberseguridad	Reputación	Legales / Regulatorios	Privacidad
🟥 5 – Catastrófico	Pérdida > 5% de ingresos anuales o quiebra.	Interrupción > 5 días o pérdida total de capacidad operativa.	Falla masiva o pérdida completa de infraestructura crítica.	Exfiltración masiva de datos, ransomware total o crisis de disponibilidad.	Crisis reputacional internacional, pérdida de clientes clave o confianza pública.	Sanción severa, suspensión de licencia, demandas o acción penal.	Exposición masiva de datos personales o sensibles con sanción y pérdida de confianza institucional.
🟧 4 – Alto	Pérdida entre 3% y 5% de ingresos.	Interrupción 3–5 días con impacto significativo en clientes o servicios.	Caída prolongada de sistemas esenciales.	Brecha de datos sensibles o cifrado generalizado.	Noticia nacional, pérdida notable de reputación o impacto en stakeholders.	Multa alta > 1.000 UTM o litigio relevante.	Filtración parcial de datos sensibles o denuncias ante autoridad.
🟨 3 – Moderado	Pérdida entre 1% y 3% de ingresos.	Interrupción 1–2 días o retrasos relevantes.	Falla en sistema crítico con degradación operativa.	Compromiso parcial o intento exitoso limitado de intrusión.	Noticia local o daño reputacional moderado.	Multa menor o observación formal.	Exposición limitada de datos no sensibles.
🟦 2 – Bajo	Pérdida entre 0,5% y 1% de ingresos.	Interrupción < 8 h o reprocesos menores.	Falla parcial en sistemas no críticos.	Intento de ataque detectado y contenido.	Reclamo aislado o mención negativa leve.	Observación regulatoria sin sanción.	Fuga potencial o acceso indebido contenido sin exposición pública.
🟩 1 – Muy Bajo	Pérdida < 0,5% de ingresos.	Interrupción menor < 2 h sin afectación crítica.	Falla menor o degradación temporal sin impacto al cliente.	Evento interno detectado sin afectación ni compromiso.	Sin impacto externo ni visibilidad pública.	Incumplimiento administrativo interno leve.	Sin afectación ni riesgo a la información personal.

Impactos en el Negocio visión más aplicada

Nivel de Impacto	Salud (atenciones / mortalidad)	Gastronomía (pérdida de alimentos / clientes)	Educación (clases / horas perdidas)	Telecomunicaciones (servicio y usuarios)	Minería (operacional / financiero)	Pensiones (servicio y confianza)
🟥 5 – Catastrófico	Interrupción total de servicios críticos (>60% de atenciones suspendidas) o ≥3 fallecidos.	Pérdida total de alimentos o cierre prolongado con >70% de caída en comensales.	Suspensión total de clases >5 días o pérdida del trimestre académico.	Caída nacional o >50% de usuarios sin servicio ≥6 h; interrupción de comunicaciones de emergencia.	Paralización total de faenas o pérdida ≥5% producción (>US$25M).	Interrupción total de pagos ≥12 h o inaccesibilidad a fondos; daño reputacional severo y afectación masiva a adultos mayores.
🟧 4 – Alto	Pérdida del 40–60% de atenciones o pacientes en riesgo sin fallecidos.	Pérdida del 40–70% de alimentos o cierre temporal (>3 días) con daño reputacional.	Suspensión de clases 2–5 días o pérdida >10% de horas pedagógicas.	Corte regional o degradación >30% de usuarios ≥3 h; afectación de servicios críticos (banca, salud, seguridad).	Interrupción operativa ≥1 día o pérdida 2–5% de producción (>US$10M).	**Retraso o interrupción en pagos ≥2 horas**, errores masivos en montos, accesos o acreditaciones; impacto directo en beneficiarios vulnerables.
🟨 3 – Moderado	Reducción del 20–40% de atenciones o retrasos con pacientes críticos.	Pérdida del 20–40% de alimentos o caída del 30–50% en ventas.	Suspensión parcial de clases (1 día completo) o pérdida 5–10% de horas pedagógicas.	Degradación parcial (10–30% usuarios) ≥1 h; interrupción localizada con reclamos.	Interrupción de 6–12 h o reducción parcial de operaciones (<2% producción).	**Retrasos entre 1 y 2 horas** en pagos o acreditaciones; errores aislados pero con reclamos públicos.
🟦 2 – Bajo	Reducción <20% de atenciones, sin daño clínico.	Pérdida <20% de alimentos o retraso leve.	Retraso menor o suspensión puntual de clases (<4 h).	Falla breve <1 h, impacto <10% usuarios o microcortes locales.	Interrupción <6 h, costos menores o ajuste operativo limitado.	**Retrasos menores <1 hora**, fallas puntuales o errores corregidos sin impacto al beneficiario.
🟩 1 – Muy Bajo	Afectación puntual sin impacto clínico.	Pérdida mínima sin afectar servicio.	Afectación leve sin pérdida de clases.	Degradación mínima sin reclamos.	Ajustes operativos menores, sin pérdida productiva.	Atención normal y pagos ejecutados en tiempo.

RTO y RPO

🕒 **RTO – Recovery Time Objective (Objetivo de Tiempo de Recuperación)**

Es el **tiempo máximo tolerable que un proceso o sistema puede estar fuera de servicio** antes de que cause un impacto inaceptable en la organización.

Indica **cuán rápido debe restablecerse** una función crítica después de una interrupción.

Ejemplo:

Si el sistema de pagos electrónicos de una institución tiene un RTO de **2 horas**, significa que, tras una caída, **debe volver a estar operativo dentro de esas 2 horas** para evitar pérdidas financieras o reputacionales graves.

💾 **RPO – Recovery Point Objective (Objetivo de Punto de Recuperación)**

Es la **cantidad máxima de datos que la organización está dispuesta a perder** medida en tiempo.

Define **cuán reciente debe ser la copia de respaldo** utilizada para la restauración.

Ejemplo:

Si el RPO de una base de datos de clientes es de **30 minutos**, los respaldos deben realizarse al menos cada media hora, de modo que **en caso de incidente solo se pierdan los datos ingresados en los últimos 30 minutos**.

RTO y RPO

🕒 RTO — Recovery Time Objective

- 🔹 **Qué mide:** el *tiempo máximo de inactividad tolerable*.
- 🔹 **Objetivo:** asegurar que los procesos críticos vuelvan a funcionar antes de generar pérdidas inaceptables.

Criterios para definirlo:

1. **Impacto financiero**: cuánto dinero se pierde por cada hora/minuto de interrupción.
2. **Impacto operacional**: qué tan dependiente es el proceso de sistemas o personal clave.
3. **Impacto reputacional y regulatorio**: si la demora afecta clientes, imagen o cumplimiento normativo.
4. **Disponibilidad de recursos alternos**: si existen soluciones temporales o manuales que reduzcan el impacto.

💡 **Tips clave:**

- Prioriza los **procesos críticos**: aquellos que sostienen ingresos o cumplimiento legal.
- Involucra a las áreas de negocio y TI en la definición (no lo decidas solo desde tecnología).
- **Sé realista:** un RTO demasiado corto sin infraestructura adecuada genera falsos compromisos.

💾 RPO — Recovery Point Objective

- 🔹 **Qué mide:** la *cantidad de datos que se puede perder* sin afectar gravemente la operación.
- 🔹 **Objetivo:** definir la **frecuencia mínima de respaldos o sincronización.**

Criterios para definirlo:

1. **Volumen y criticidad de los datos:** qué información se actualiza constantemente (pagos, transacciones, registros médicos, etc.).
2. **Tolerancia a la pérdida de información**: cuánto tiempo puede perderse sin comprometer operaciones o cumplimiento.
3. **Capacidad tecnológica**: infraestructura de respaldo y replicación disponible.
4. **Costo vs. frecuencia del backup**: respaldos más frecuentes implican mayores costos.

💡 **Tips clave:**

- **Evalúa el flujo de datos real:** si una base se actualiza cada 5 minutos, un RPO de 1 hora no sirve.
- Ajusta el RPO según **criticidad del sistema** (por ejemplo, bases contables vs. archivos de RRHH).
- Usa **replicación continua o incremental** para procesos críticos (banca, salud, pensiones).

Ejemplos de BIA

Ejemplo de Análisis de Criticidad de Procesos

Nombre del Proceso	Categoría de Impacto	0-30 minutos	30 minutos 2 horas	2-6 horas	6 horas 1 día	1 - 3 días	3 días 1 semana	Mayor a 1 semana	Justificación y Comentarios
Pago de Remuneraciones	FINANCIERO								A partir del 4° día es posible replicar la base del mes anterior
	REPUTACIONAL								
	REGULATORIO								
	SEGURIDAD/ SALUD								
	RESULTADO								
	RTO (Objetivo de Tiempo de Recuperación)	1 - 3 días							

Nombre del Proceso	Categoría de Impacto	0-30 minutos	30 minutos 2 horas	2-6 horas	6 horas 1 día	1 - 3 días	3 días 1 semana	Mayor a 1 semana	Justificación y Comentarios
Pago de Pensiones	FINANCIERO								Tiempo máximo de espera en sucursal no puede superar las 2 horas.
	REPUTACIONAL								
	REGULATORIO								
	SEGURIDAD/ SALUD								
	RESULTADO								
	RTO (Objetivo de Tiempo de Recuperación)	30 minutos – 2 horas							

Análisis RIA (Risk Analysis)

Objetivos del RIA (Risk Analysis):

- Identificación, evaluación y valorización de los riesgos de los procesos, centrándose en aquellos que podrían afectar la continuidad del negocio.

- Tratamiento de la incertidumbre, dada por factores internos como externos.

- Proveer la información base que permitirá determinar las estrategias de recuperación más apropiadas.

Resultados del RIA:

- Introducción al Análisis de Riesgo (RIA)
- Identificación y evaluación de las amenazas que pueden afectar a la organización.
- Estimación del riesgo inherente asociado a cada amenaza.
- Identificación valorización de los controles asociados a cada riesgo identificado.
- Estimación del riesgo residual asociado a cada amenaza.
- Se deberá gestionar la necesidad de generar planes de acción para mitigar los riesgos.

¿Cuáles contextos de riesgos es más probable que afecte la continuidad?

Panorama de Amenazas 2024 - ENISA

Análisis de Criticidad de Procesos

- En la ISO 22.317 dentro de la cláusula 5.4 Priorización de los procesos, define los siguientes requisitos.

- 5.4.1 Generalidades
- "Un proceso es un conjunto de actividades que de interrelacionan o interactúan y que transforman los elementos de entrada en resultados (ISO 22.300). Su prioridad viene determinadas por la prioridad de los productos y servicios que constituyen su resultado"

- 5.4.2 Elementos de entrada
  - La información requerida para la priorización de los procesos incluye lo siguiente:
  - El alcance del BIA (servicios, productos).
  - Los requisitos de entrega de productos y prestación de servicios (plazos, calidad, cantidad, niveles de servicios y especificaciones sobre la capacidad).
  - Los procesos y productos que entrega el negocio y servicios que se prestan mediante ellos.
  - Los impactos en el tiempo ante la no entrega de los productos o servicios 3 (RTO).

8.3 Estrategias de Continuidad (ISO 22.301)

- 8.3.1 Generalidades
- La organización debe identificar y seleccionar estrategias de continuidad del negocio que consideren opciones para antes, durante y después del evento disruptivo basadas en los resultados de los análisis de impacto en el negocio y evaluación del riesgo. Las estrategias de continuidad del negocio deben componerse de una o más soluciones.

- 8.3.2 Identificación de estrategias y soluciones
- La identificación de estrategias y soluciones debe basarse en la medida que estas:
  a) Cumplan con los requisitos para continuar y recuperar actividades prioritarias dentro de los plazos identificados y la capacidad acordada.
  b) Consideren la cantidad y el tipo de riesgo que se puede o no aceptar.
  c) Consideren los costos y beneficios asociados

Ejemplos en Personas

Tiempo mínimo de recuperación efectivo	Ejemplos de opciones de estrategias	Requisitos previos
En el plazo de una hora	Otro personal del mismo emplazamiento con las destrezas/capacidades requeridas se hace cargo de la actividad	– Proporcionar formación cruzada al personal que trabaja en un mismo emplazamiento – Documentar los procesos de negocio normales
	El personal de un emplazamiento no afectado con las destrezas/capacidades requeridas se hace cargo de la actividad al trasladarse esta a un emplazamiento no afectado	– Proporcionar formación cruzada al personal que trabaja en un emplazamiento alternativo – Documentar los procesos de negocio normales
	Planificar la sucesión para los roles esenciales	– Designación y formación de sustitutos
	Disponer de personas alternativas con autoridad delegada	– Designar directores y otorgarles autoridad delegada
En el plazo de unas horas	Confirmar la presencia en el emplazamiento de otro personal con las destrezas/capacidades requeridas que puede hacerse cargo de la actividad	– Proporcionar formación cruzada al personal que trabaja en emplazamientos, centros y regiones diferentes – Separar geográficamente al personal que tenga las mismas destrezas
	Transferir los roles a proveedores o contrataciones externas	– Los recursos con las destrezas requeridas provistos por un proveedor externo se encuentran en el emplazamiento y pueden hacerse cargo de la actividad – Establecer y preparar los procesos para transferir (o contratar externamente) la actividad a un tercero o un proveedor externo
	Contratar a personas externas con las destrezas requeridas	– Identificar a los proveedores externos capaces de proveer el conjunto de destrezas requerido

Tiempo mínimo de recuperación efectivo	Ejemplos de opciones de estrategias	Requisitos previos
En el plazo de unos días	Designar a personal disponible en el emplazamiento de actividades que pueden tolerar un tiempo de inactividad y formarle antes de realizar la transición del trabajo	– Elaborar material de formación para cada conjunto de destrezas e impartir la formación al personal designado
	Designar a personal de emplazamientos no afectados de actividades que pueden tolerar tiempo de inactividad y formarle antes de realizar la transición del trabajo	– Elaborar material de formación para cada conjunto de destrezas e impartir la formación al personal designado – Establecer criterios de selección de personal
En el plazo de una semana	Contactar con antiguos empleados y celebrar contratos de corta duración	– Mantener listas de antiguos empleados con las destrezas necesarias
	Buscar y contratar personal temporal/subcontratado a través de agencias externas	– Elaborar material de formación para cada conjunto de destrezas e impartir la formación al personal designado a su llegada a las instalaciones
En el plazo de semanas o meses	Contratar personal de sustitución en el mercado a través de agencias externas	Ninguno
	Contratar personal de sustitución reclutado de la competencia a través de agencias externas	Ninguno
NOTA Para obtener más información, véase la Especificación Técnica ISO/TS 22330.		

Ejemplos en Edificios y Servicios

Tiempo mínimo de recuperación efectivo	Ejemplos de opciones de estrategias	Requisitos previos
En el plazo de una hora	Dividir el trabajo de la actividad entre varios emplazamientos	– Operar la actividad en otro(s) emplazamiento(s) en todo momento
	Tener la capacidad y las destrezas para transferir la actividad a otro emplazamiento	– Realizar la transferencia del trabajo periódicamente para mantener la capacidad
	Preparar y activar tecnología de sustitución de servicios públicos *in situ* (por ejemplo, un grupo electrógeno, energía solar, etc., en el emplazamiento)	– Instalar capacidades de autogeneración o cogeneración (por ejemplo, un grupo electrógeno en el emplazamiento)
En el plazo de un día	Desplazar las actividades de menor prioridad (con un RTO más largo) por personal de actividades de alta prioridad (con un RTO más corto) en el propio centro de trabajo	– Acordar con los departamentos afectados las prioridades de desplazamiento y la ubicación de las personas desplazadas en el propio centro de trabajo
	Reconfigurar los edificios o el entorno de trabajo (por ejemplo, salas de juntas o cafetería) dentro de la ubicación	– Realizar trabajos preparatorios o elaborar planes para facilitar esta situación
En el plazo de unos días	Desplazar las actividades de menor prioridad (con un RTO más largo) con personal de actividades de alta prioridad (con un RTO más corto) en otro emplazamiento	– Documentar las preferencias priorizadas para las áreas de trabajo alternativas y acordarlas con los departamentos afectados – Considerar los problemas de personal al realizar una reubicación – Identificar los recursos adicionales que se requieren para reiniciar la actividad en el emplazamiento alternativo
	Reconfigurar los edificios o el entorno de trabajo (por ejemplo, salas de reuniones o cafetería) de un emplazamiento, centro de trabajo o región externos para la reubicación o transferencia y, a continuación, poner en marcha las instalaciones	– Documentar las preferencias priorizadas de áreas de trabajo alternativas externas – Considerar los problemas de personal al realizar una reubicación – Identificar los recursos adicionales que se requieren para reiniciar la actividad
	Reubicar la actividad en las instalaciones de un socio comercial o de un proveedor de servicios de recuperación de áreas de trabajo	– Establecer un acuerdo con otra organización o contratar a un proveedor externo de servicios de recuperación de áreas de trabajo
	Reubicar la actividad en el propio domicilio del personal	– Inspeccionar el área o espacio de trabajo de cada vivienda designada para confirmar que cumple las políticas de seguridad y salud pertinentes – Confirmar la cobertura por una póliza de seguros y la responsabilidad
	Contratar el suministro temporal de servicios públicos	– Contratar acuerdos de nivel de servicios (SLA) para el suministro de electricidad, agua, calefacción o iluminación

Ejemplos en Instalaciones

Tiempo mínimo de recuperación efectivo	Ejemplos de opciones de estrategias	Requisitos previos
En el plazo de una hora	Dividir la capacidad en el emplazamiento entre dos o más equipos	– Mantener capacidad de reserva para cada operación
	Iniciar de inmediato una solución provisional para la pérdida de los equipos o consumibles	– Documentar y preparar todos los recursos adicionales que se requieren para las soluciones alternativas – Ensayar las soluciones alternativas de forma periódica
	Utilizar las existencias *in situ* de consumibles	– Mantener existencias suficientes de consumibles *in situ*, teniendo debidamente en cuenta: – el tiempo que las necesidades estarán cubiertas con el material en stock; – los plazos de entrega del proveedor.
En el plazo de unos días	Almacenar equipos de repuesto *in situ*	– Tener un plan para instalar y poner en servicio equipos de repuesto con el fin de cumplir los plazos requeridos
	Preparar y, en su momento, iniciar una solución alternativa para la pérdida de equipos o consumibles	– Identificar las opciones de soluciones alternativas y todos los recursos requeridos
	Llevar a cabo una actividad de recuperación para recobrar los equipos y consumibles del emplazamiento afectado	– Investigar soluciones contractuales o de suscripción con empresas especializadas en restitución de activos o consultar a especialistas en recuperación para obtener asesoramiento con antelación
	Se utilizan existencias de consumibles de otra ubicación	– Mantener existencias suficientes de consumibles en otro emplazamiento o región, teniendo debidamente en cuenta: – el tiempo que las necesidades estarán cubiertas con el material en stock; – el tiempo que se tarda en entregar los artículos desde el emplazamiento externo.

Tiempo mínimo de recuperación efectivo	Ejemplos de opciones de estrategias	Requisitos previos
En el plazo de unos días o semanas (según los equipos de que se trate)	Reubicar y poner en servicio equipos de repuesto instalados o almacenados en otra ubicación	– Asegurarse de que haya equipos de repuesto almacenados en otra ubicación y de que se puedan reubicar y poner en servicio en el tiempo disponible
	Solicitar, alquilar u obtener en régimen de leasing equipos de repuesto de un proveedor	– Documentar un plan de instalación
	Reparar los equipos deteriorados	– Contratar un acuerdo de mantenimiento con un proveedor que cubra los daños por incidentes
	Solicitar consumibles de repuesto a un proveedor	– Tener en cuenta los plazos de entrega
En el plazo de unos meses	Adquirir equipos nuevos	– Mantener un registro de los equipos disponibles, cambios en las especificaciones e información de contacto de los proveedores

Ejemplos en TICs

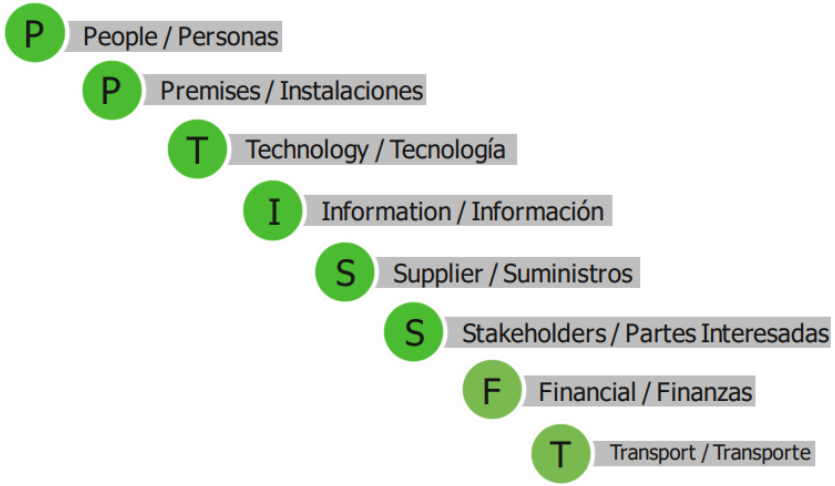
Tiempo mínimo de recuperación efectivo	Ejemplos de opciones de estrategias	Requisitos previos
En el plazo de una hora	Replicar el sistema de aplicaciones y tenerlo activo en otra plataforma, que puede denominarse un sistema «en caliente» o «activo/activo». Los datos de las dos plataformas, unidades de red y/o matrices de almacenamiento se sincronizan en tiempo real.	– Establecer sistemas replicados en dos o más emplazamientos que estén bien alejados entre sí: – propiedad de la organización; o – mediante contratos y acuerdos de nivel de servicio con un proveedor externo de servicios de alojamiento. – Identificar los plazos de reconfiguración (de haberlos) si se pierde uno de los emplazamientos y ensayarlos con periodicidad
	Replicar los enlaces de comunicaciones de datos y los dispositivos de comunicaciones (por ejemplo, enrutadores, conmutadores o módems) Utilizar un enrutamiento divergente de las comunicaciones de datos	– Implementar un enrutamiento divergente replicado de los enlaces de redes LAN y WAN – Instalar la redundancia en los dispositivos de comunicación
	Redireccionar de manera automática o mediante un servicio externo las comunicaciones de voz a otros emplazamientos	– Contratar servicios de telefonía gestionados externamente, que pueden utilizarse para la actividad normal y reconfigurarse durante el incidente

Tiempo mínimo de recuperación efectivo	Ejemplos de opciones de estrategias	Requisitos previos
En el plazo de unos días	El sistema de aplicaciones se ha precargado en otra plataforma y requiere mantenimiento o actualizaciones para ser pareja a la versión de producción Los datos de aplicaciones requieren restauración a partir del registro de transacciones o de la copia de seguridad más reciente, lo que suele denominarse «sistemas auxiliares en caliente» Se aloja el servicio en otro centro de datos de la propia organización o en las instalaciones de un proveedor externo de servicios de TIC	– Crear una copia del sistema de aplicaciones en una plataforma alternativa – Establecer un proceso que transfiera las copias de seguridad de los datos a una ubicación que sea accesible para el lugar en el que está ubicada la plataforma alternativa – Realizar ensayos periódicos del proceso de restauración de datos, sobre todo después de las actualizaciones de sistemas
	Sustituir los equipos de sobremesa mediante un servicio contratado externamente; el proveedor puede preconfigurar los equipos antes de entregarlos	– Asegurarse de que el proveedor tenga las configuraciones requeridas de los equipos de sobremesa
	Se replican los enlaces de comunicaciones de datos Sustituir los dispositivos de comunicaciones (por ejemplo, enrutadores, conmutadores o módems) por dispositivos de repuesto almacenados *in situ* o en otra ubicación Instalar redes inalámbricas para cubrir nuevas áreas de trabajo	– Mantener un conjunto de dispositivos de red y comunicaciones compatibles

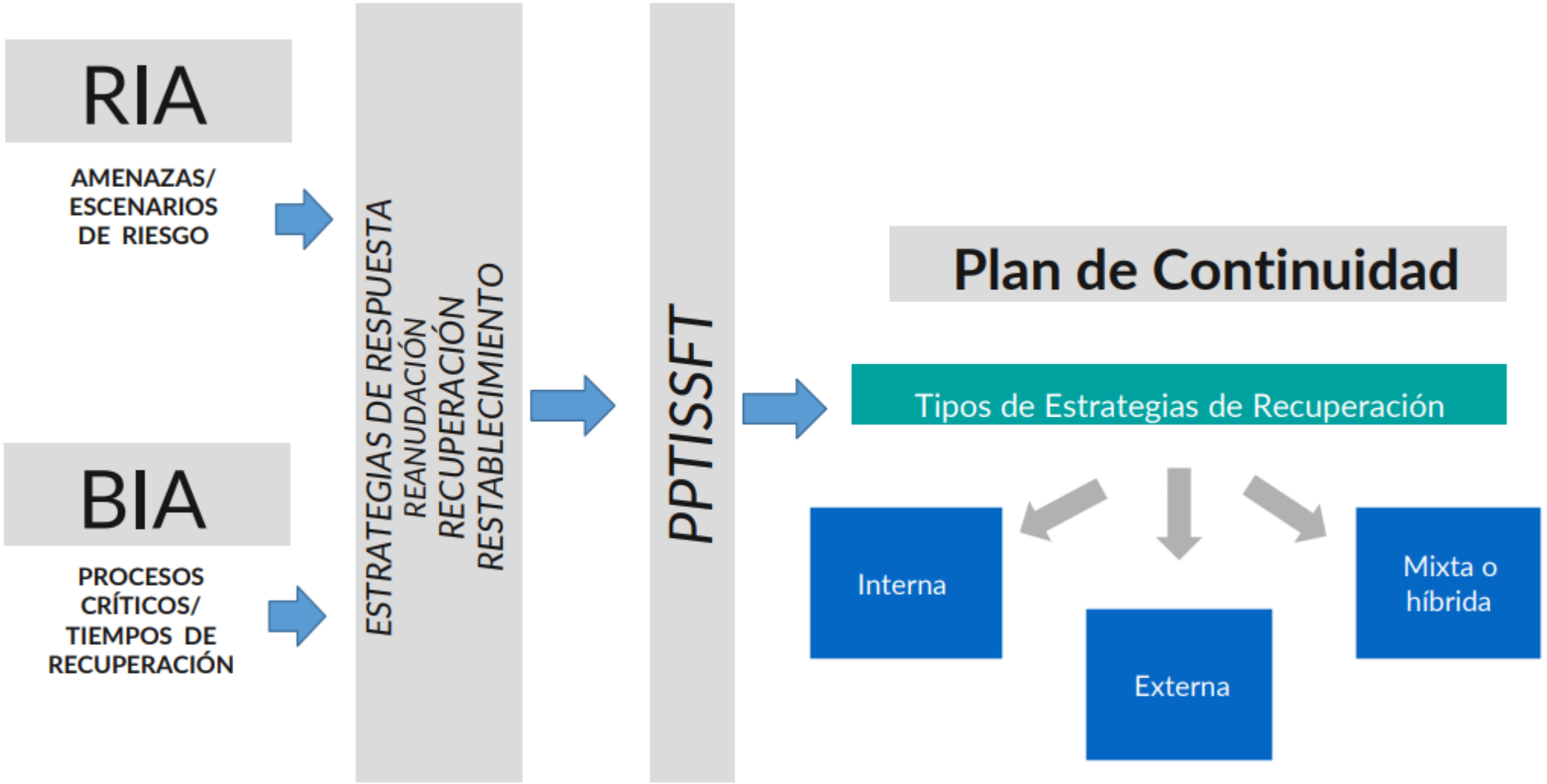
8.3.2 Determinación de los requisitos de los recursos

- La organización debe determinar los requisitos de los recursos para implementar las estrategias seleccionadas. Los tipos de recursos deben incluir, pero no limitarse, a:

  - a) Personas
  - b) Información y datos
  - c) Edificios, ambiente laboral y servicios asociados
  - d) Instalaciones, equipos y productos de consumo
  - e) Sistemas de tecnología de la información y comunicación (TIC
  - f) Transporte
  - g) Financiamiento
  - h) Socios y proveedores.



Contexto General



Planes y procedimientos de continuidad del negocio

- En la ISO 22.301 dentro de la cláusula 8.4 Planes y procedimientos de continuidad del negocio, podemos encontrar los siguientes requisitos.

- **8.4.1 Generalidades**

- Las organizaciones deben implementar y mantener esquemas de respuesta que permitan una **alerta a tiempo** y la comunicación a las partes interesadas pertinentes.

- Debe proporcionar planes y procedimientos para gestionar la organización **durante una disrupción**. Los planes y procedimientos deben usarse cuando sea pertinente para activar las soluciones de continuidad del negocio.

- La organización debe identificar y documentar los planes y procedimientos de continuidad del negocio basados en el resultado de las **estrategias** y soluciones seleccionadas.

Consideraciones procedimientos de continuidad del negocio

1. Portada y Control de Documento

- Título, versión, fecha de emisión, propietario del documento.
- Número de control, clasificación de seguridad, firmas de aprobación.
- Historial de revisiones.

2. Propósito y Alcance

- Objetivo general del plan.
- Procesos, sistemas, instalaciones y áreas incluidas.
- Exclusiones y límites (por ejemplo, servicios de terceros).

3. Contexto y Marco de Referencia

- Relación con políticas corporativas, ISO 22301, ISO 27001, o regulaciones locales (CMF, INN, etc.).
- Supuestos y dependencias críticas (infraestructura, proveedores, personas).

4. Análisis de Impacto y Evaluación de Riesgos (BIA y BRA)

- Resumen de los procesos críticos identificados.
- RTO (Tiempo Máximo de Recuperación) y RPO (Pérdida Máxima de Datos).
- Escenarios de interrupción y sus impactos cuantificados.

5. Roles y Responsabilidades

- Comité de crisis, coordinador de continuidad, CISO, CIO, comunicaciones, legal, RRHH, etc.
- Líneas de reporte, suplentes y datos de contacto.

6. Procedimientos de Activación del Plan

- Criterios para declarar una emergencia o incidente.
- Mecanismos de notificación y comunicación (interna y externa).
- Autoridad para activar el plan y procesos de escalamiento.

7. Estrategias y Procedimientos de Continuidad

- Acciones inmediatas post-incidente (primeras 2 horas).
- Procedimientos por proceso crítico.
- Sitios alternos, trabajo remoto, respaldo de infraestructura, proveedores de contingencia.

8. Plan de Recuperación Tecnológica (DRP)

- Estrategias de restauración de sistemas y datos.
- Procedimientos técnicos por entorno (on-premise, nube, comunicaciones, aplicaciones críticas).
- Secuencia de priorización de sistemas y validaciones post-restauración.

9. Plan de Comunicación y Gestión Reputacional

- Canales oficiales, mensajes tipo, voceros designados.
- Comunicación con empleados, clientes, medios y reguladores.
- Plantillas de comunicados de emergencia.

10. Pruebas, Ejercicios y Mantenimiento

- Tipos de ejercicios (técnicos, simulados, integrales).
- Frecuencia mínima (anual o semestral).
- Registro de resultados, lecciones aprendidas y mejoras.

Buenas Practicas de un BCP

1. 🧩 Estructura modular y clara

Redacta el BCP por secciones independientes (activación, roles, comunicación, recuperación).
Esto permite **activar solo lo necesario** según el tipo de incidente, sin tener que revisar todo el documento.

2. 👥 Define backups de personas y cargos

Por cada rol crítico, designa **un titular y un suplente entrenado**, con datos actualizados.
Evita depender de una sola persona: *"Cada función crítica debe tener al menos un reemplazo competente."*

3. 📞 Comunicación interna inmediata

Incluye una **cadena de comunicación escalonada** (quién avisa a quién) con medios alternativos: teléfono fijo, celular, correo, chat corporativo y WhatsApp.
💡 *Tip:* Añade plantillas breves de mensajes de emergencia.

4. 💬 Lenguaje directo y sin ambigüedades

Usa verbos de acción y evita tecnicismos excesivos:

- Mejor: "El Coordinador debe activar el plan dentro de 15 minutos".
- Peor: "Se espera que el plan sea activado en un tiempo razonable".

5. 📄 Formatos y checklists operativos

Cada procedimiento debe tener un **checklist o formulario** que permita registrar decisiones y acciones en tiempo real (quién, cuándo, cómo).
Así garantizas trazabilidad y evaluación posterior.

6. 🧑‍🏫 Formación y entrenamiento continuo

Todo el personal con rol en el BCP debe recibir **formación práctica anual**, con ejercicios y simulaciones.
Capacita también a los suplentes y a las áreas de soporte (TI, RRHH, comunicaciones).

7. 🔄 Pruebas progresivas y realistas

Comienza con ejercicios de escritorio (*table-top*) y avanza a simulacros integrales.
Evalúa resultados y **ajusta el plan** según las lecciones aprendidas.

8. 🔐 Protege y controla el documento

Guarda el BCP en formato digital seguro (PDF protegido y copia cifrada en la nube) y en versión física sellada.
Evita versiones no controladas: implementa una **tabla de control documental**.

9. 🧭 Versiona y actualiza por cambios reales

Actualiza el BCP cada vez que cambie la estructura, tecnología o liderazgo.
Indica versión, fecha y responsables de revisión: *"Versión 3.2 – Revisada 07/11/2025 por Coordinador BCM"*.

10. 💡 Redacción centrada en la acción y la claridad visual

Usa **cuadros, diagramas, íconos o flujos** para facilitar la comprensión en crisis.
Un BCP debe **poder leerse y ejecutarse bajo presión**, incluso con estrés o sin conectividad.

Ejemplos base dentro del BCP

⚠️ Ejemplo: Plan de Activación del BCP

Objetivo

Establecer el procedimiento para declarar y activar el Plan de Continuidad del Negocio ante una interrupción significativa que afecte procesos o servicios críticos.

Criterios de Activación

- Interrupción de servicios críticos por más de **30 minutos** sin solución inmediata.
- Indisponibilidad de infraestructura, sistemas o personal esencial.
- Confirmación de incidente mayor por parte del **Comité de Crisis o CISO**.

Procedimiento

1. **Detección y notificación:**
   Cualquier colaborador que detecte el incidente informa de inmediato al **Coordinador de Continuidad**.
2. **Evaluación inicial:**
   El Coordinador evalúa el alcance y propone la activación al **Líder de Crisis**.
3. **Decisión de activación:**
   El Líder de Crisis autoriza formalmente la activación del plan.
4. **Comunicación oficial:**
   Se notifica al Comité de Crisis, Alta Dirección y áreas críticas.
5. **Ejecución:**
   Se ponen en marcha los procedimientos de recuperación definidos (sitios alternos, respaldos, comunicación, etc.).
6. **Registro:**
   Todas las acciones se documentan en la **Bitácora de Incidente BCP**.

🗣️ Ejemplo: Plan de Comunicación en Crisis

Objetivo

Asegurar una comunicación clara, oportuna y coherente con todos los públicos durante una situación de crisis o activación del BCP.

Principios

- Transparencia controlada: comunicar hechos verificados.
- Coherencia: mantener un solo vocero y mensaje unificado.
- Prioridad humana: proteger a las personas antes que la imagen.

Roles Clave

- **Vocero Oficial:** Gerente General o Líder de Crisis.
- **Canal Interno:** Comunicaciones internas / RRHH.
- **Canal Externo:** Encargado de Comunicaciones con medios y clientes.

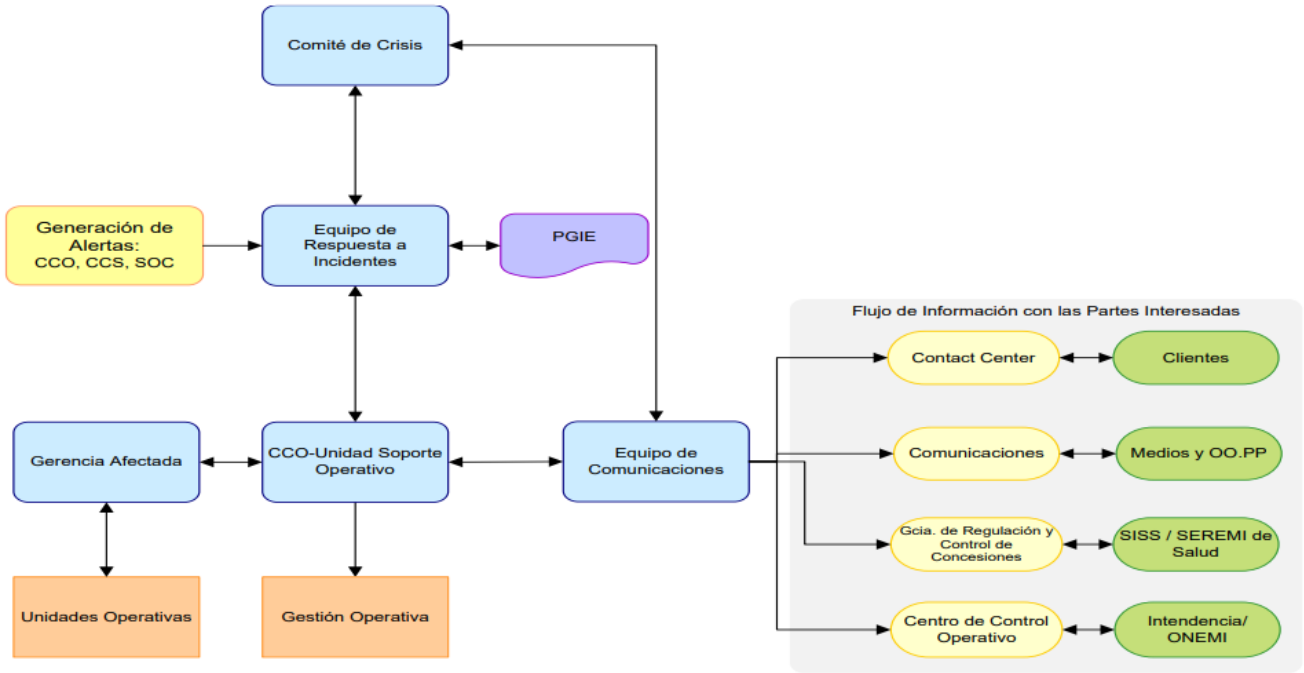
Flujo de Comunicación

1. **Mensaje inicial interno:**
   Se informa a los colaboradores sobre la naturaleza del incidente, medidas adoptadas y canales de actualización.
2. **Mensaje externo:**
   Comunicado breve a clientes o medios (solo con aprobación del Comité de Crisis).
3. **Actualizaciones periódicas:**
   Cada 60 minutos o según evolución del evento.
4. **Cierre del incidente:**
   Mensaje de normalización y agradecimiento, seguido de informe post-evento.

8.4.2 Esquemas de respuesta

- La organización debe implementar y mantener una estructura e identificar uno o más equipos responsables para responder a las disrupciones.

- Los roles y responsabilidades de cada equipo y las relaciones entre otros equipos deben estar claramente establecidas.



Ejercicios y Pruebas de los Planes

- Validar la capacidad de recuperarse de la organización.
- Asegurar que los procedimientos sean apropiados e identificar deficiencias existentes.
- Entrenar a los equipos y partes interesadas.
- Proporcionan un mecanismo para mantener los planes actualizados.
- Permiten mantener informada a la Alta Administración.

Programación y coordinación de pruebas:

- Programar la prueba durante un tiempo que minimice las interrupciones a las operaciones normales.
- Especificaciones: Tipo de prueba, alcance, participantes, logística, ambiente de control, seguridad.
- Tiempo de ejecución de la prueba: Día, hora, duración, punto de retorno.
- Documentación y análisis de los resultados.
- Mantenimiento de los Planes.

Ejercicios y Pruebas de los Planes

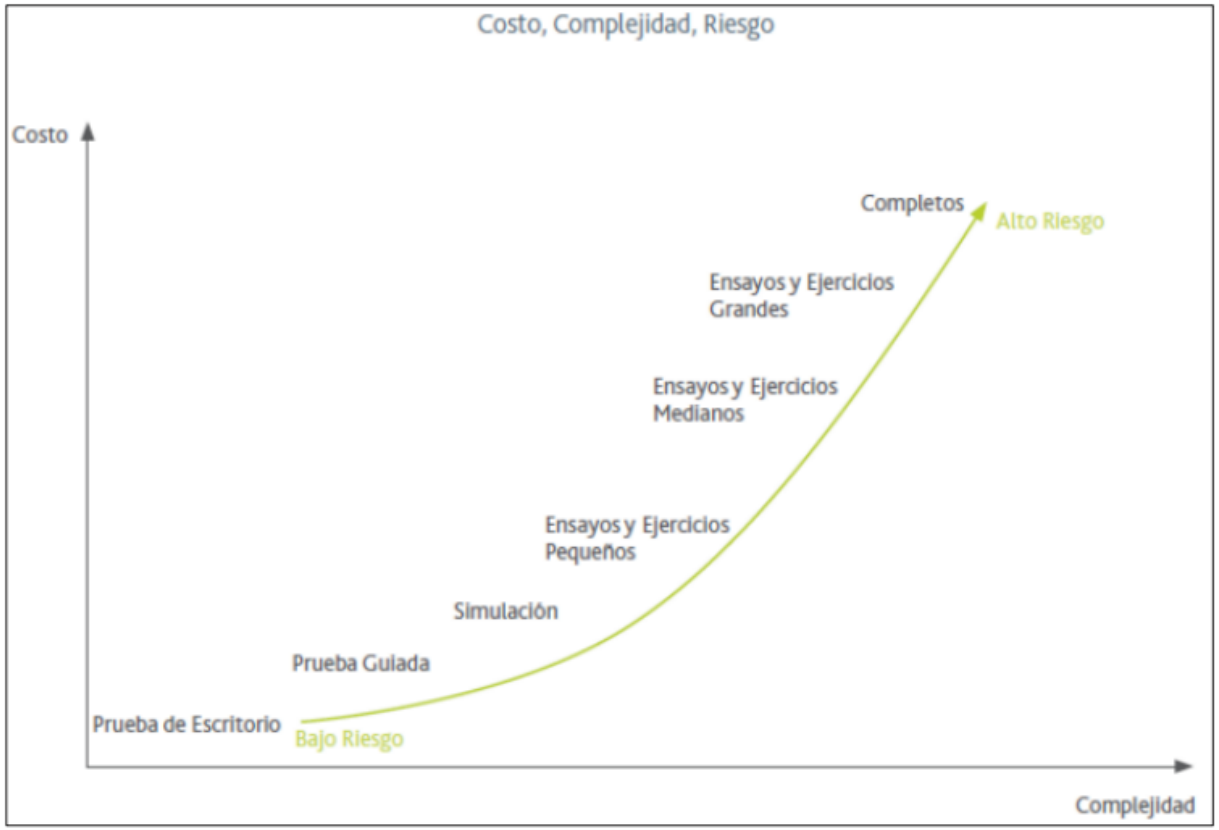
Nivel de Criticidad del proceso (Evaluación BIA)	Frecuencia
Muy Alto / Alto	Cada 12 meses (o cuando existe un cambio significativo en el BCP)
Medio	Cada 24 meses (o cuando existe un cambio significativo en el BCP)
Bajo	Cada 36 meses (o cuando existe un cambio significativo en el BCP)

Ejemplo requerimientos de prueba por nivel de criticidad

Tipo de Ejercicio	Nivel de Criticidad del Proceso			
	Muy Alto	Alto	Medio	Bajo
1. Escritorio				
2. Simulación y/o Conectividad				
3. Test Integrado				
4. Test en vivo				

Ejercicios y Pruebas de los Planes

- Asemejarse a la realidad.
- No debe interrumpir actividades normales de trabajo.
- Preparar planes escritos de las pruebas (no improvisar).
- Preparar la programación de pruebas de largo plazo.
- Comenzar en forma simple, crecimiento gradual.
- Buscar debilidades.
- Validar tiempos.
- Aprender de los resultados.
- Esperar errores y problemas, documentando para buscar soluciones.
- Probar sobre una misma documentación.



Proceso de Gestión de Continuidad del Negocio

Marco	Control / Sección relevante	Qué aporta
ISO 27001:2022	**Cláusula 8.5** Gestión de Continuidad de la Información	Exige que la organización mantenga operación durante incidentes.
ISO 27002:2022	**5.29 y 5.30** (Continuidad y Redundancia)	Define cómo proteger disponibilidad y recuperar operaciones.
ISO 22301:2019 (BCM)	**Cláusulas 8.2 – 8.4** (BIA, Estrategias, Ejercicios)	Marco completo para resiliencia organizacional.
CIS Controls v8.1	**Control 11 – Data Recovery**	Asegura recuperación de datos confiable, probada y segura.
NIST SP 800-53 r5	**CP-1 a CP-10** (Contingencia y recuperación)	Requisitos técnicos para recuperación de servicios e infraestructura.
NIST SP 800-34 r1	**Contingency Planning Guide**	Guía práctica para estructurar planes y pruebas.
COBIT 2019	**DSS04 – Continuidad de Servicio**	Enmarca el gobierno y ciclo de vida de la continuidad.

- 22.300 – Vocabulario
- 22.301 – Requisitos del sistema de gestión de continuidad del negocio
- 22.313 – Directrices de Implementación
- 22.317 – Directrices para el desarrollo del BIA
- 22.320 – Directicas para la respuesta a incidentes
- 22.331 - Directrices para estrategias de continuidad del negocio
- 22.332 – Directrices para la implementación de planes de continuidad
- 22.398 – Directrices para el desarrollo de ejercicios

La Integración con la Protección de Datos

La protección de datos, el gobierno de datos y la inteligencia artificial son nuevos desafíos criticos

[Workshops 2025 • Diplomados en Ciberseguridad]

CAPACITACIÓN USACH
UNIVERSIDAD DE SANTIAGO DE CHILE

Gestión de Incidentes y Continuidad Operacional

Workshop N°3: Experiencias prácticas y aplicación con Ley Marco de Ciberseguridad

ALIGNMENT
SOLUCIONES ESTRATÉGICAS

DIPLOMADO
CIBERSEGURIDAD