12 MARZO 2021

II CONGRESO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

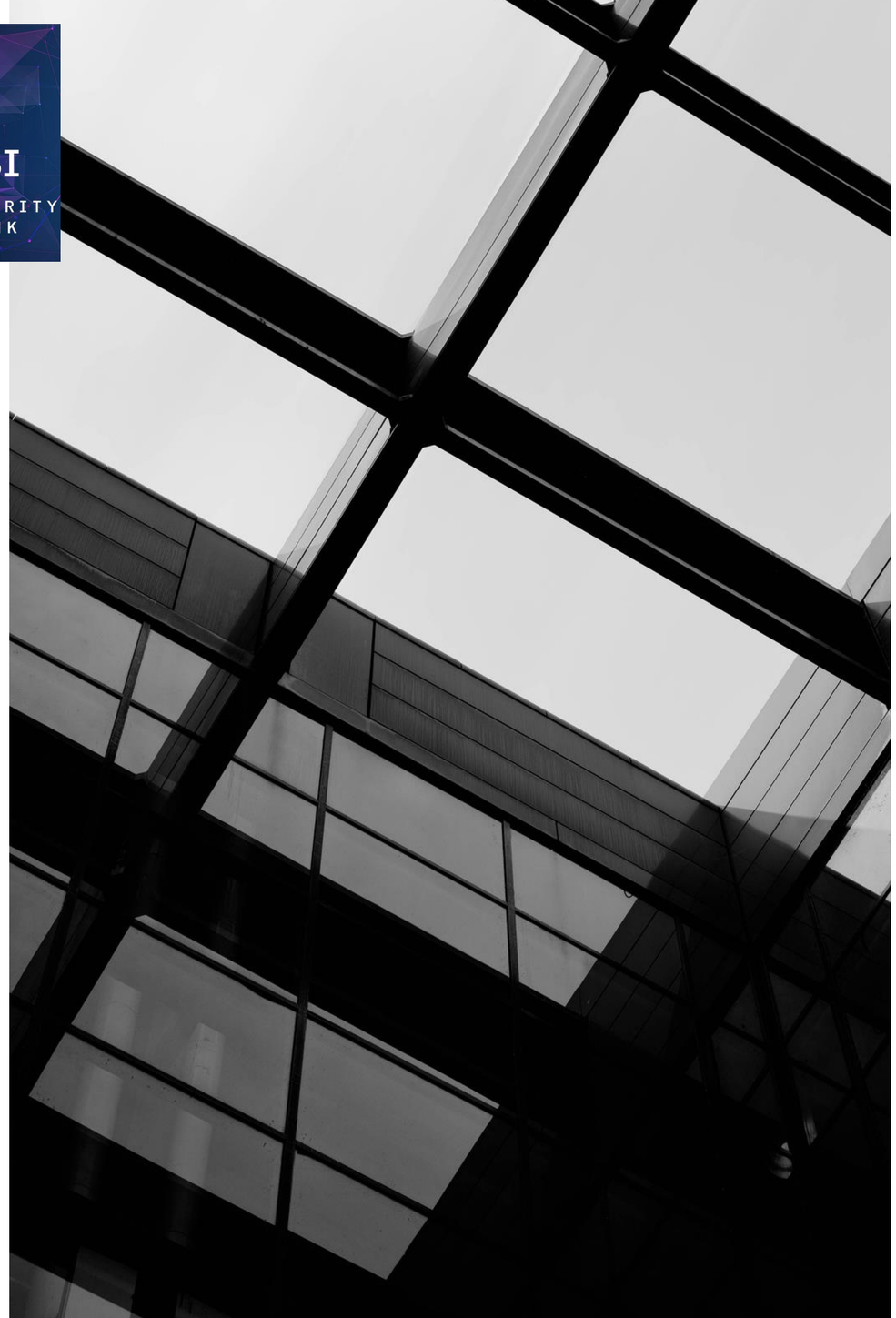
“Estrategias de Continuidad del Negocio”

SOCHISI
DIGITAL SECURITY THINK TANK

Speaker:
Cristian Maldonado Urrutia

Linkedin
www.linkedin.com/in/cmaldonadou

SOCHISI.CL/ENVIVO



¡Bienvenidos a la charla!

Agenda de hoy

01 Conceptos claves

02 Ejemplos de Indisponibilidad de recursos de la Organización

03 ISO 22331:2020 “Directrices para Estrategias de Continuidad”.

04 En concreto ¿Qué nos propone ISO 22331:2020?

05 Consideraciones Finales

Estrategias de Continuidad del Negocio

Seguridad y Resiliencia ISO 22331

¿Qué hacer cuando el escenario de contingencia se convierte en un escenario de normalidad?

¿Qué debemos hacer cuando nuestra estrategia de continuidad de corto plazo se convierte en una estrategia de Largo Plazo?

Conceptos claves

Continuidad de Negocio	“Capacidad de la Organización para continuar entregando productos o servicios a niveles predefinidos aceptables, tras un incidente que genere una interrupción“ ISO 22300.
Estrategia de Continuidad de Negocio	“Acciones necesarias para abordar los resultados del Análisis de Impacto en el Negocio (BIA) y la Evaluación de Riesgos para cumplir con los objetivos de continuidad de negocio” ISO 22313.
Resiliencia	“Capacidad de adaptación de una organización en un entorno complejo y cambiante” ISO 22300.

Ejemplo 1: Personas

Indisponibilidad de Personal

Reasignación de funciones

Contratación de personal de apoyo

Ejemplo 2: Instalaciones

Indisponibilidad de Instalaciones

Realocación en otras instalaciones

Teletrabajo

Ejemplo 3: Información y Datos

Indisponibilidad de la Información

Replicación de datos

Proveedor de Servicio Externo

1.- ¿Qué hacer cuando el escenario de contingencia se convierte en un escenario de normalidad?

Personas

La indisponibilidad del personal de la empresa se puede prolonger por más tiempo del esperado:

- Contagio y medidas de seguridad y salud de gobierno (Pandemia, estados de emergencia, ausencia de transporte seguro, regreso a clases).
- Seguridad de la Sociedad, estallidos sociales, movilizaciones, protestas y falta de un entorno Seguro para trabajar.
- Ausencia de tecnología y herramientas de comunicación apropiadas para el Desarrollo de funciones.

Información y Datos

- Sistemas de información vulnerables, amenazas digitales, entornos legales cambiantes (inversion obligatoria en ciberseguridad).
- Menor oferta de proveedores se servicios TI, tiempos de implementación muy extensos.
- Transformación digital “forzada”.

Instalaciones

- Costo y viabilidad de la reconstrucción.
- Búsqueda de entornos más seguros.
- Redefinición de los servicios/productos.

2.- ¿Qué debemos hacer cuando nuestra estrategia de continuidad de corto plazo se convierte en una estrategia de Largo Plazo?

Personas

La reasignación personal de la empresa a funciones críticas, en el Largo Plazo no será una estretagia efectiva:

- Con el tiempo funciones y procesos que negocio que no eran tan críticos, se empiezan a convertir en críticos.
- El sobretrabajo y exceso de horas estraordinarias de trabajo generará problemas de salud en el personal (stress, ansiedad, depresión) y afectará la calidad del trabajo.
- La necesidad de realizar muchas tareas durante la jornada, descuidará focos relevantes como la seguridad de la información, riesgo operacional y auditoria.

Información y Datos

- Un proceso periódico de réplica y recuperación de datos requiere de horas de personal técnico calificado (recursos limitados, sobretodo en un contexto de contingencia).
- Pérdida de foco en la Seguridad de la Información.
- Un proveedor con exceso de demanda podría no asegurar la disponibilidad de la información.

Instalaciones

- Espacios que requieren volver a su definición original (oficinas, salas de reunion, cafeterias).
- Personal utilizando recursos propios (falta de entorno seguro, disponibilidad, riesgos de ciberseguridad).

ISO 22331:2020 “Directrices para la Estrategia de Continuidad de Negocio”

“No hay una formula mágica. Las estrategias de continuidad de negocio dependerán de los objetivos, naturaleza y recursos propios de cada Organización”.

ISO 22331:2020 nos entrega algunas directrices generales para definer de major manera estas estrategias.

ISO 22331:2020

La determinación y selección de estrategias debe incluir:

PROTEGER

Proteger las actividades priorizadas

CONTINUAR

Estabilizar, continuar, reanudar y recuperar las actividades priorizadas.

GESTIONAR

Mitigar, responder y gestionar los impactos

ISO 22331:2020

Elementos de la gestion de la continuidad del negocio

SOCHISI
DIGITAL SECURITY THINK TANK

ISO 22331 plantea que las estrategias de continuidad de negocio deban incluir:

1. Medidas para intentar reducir la frecuencia de los incidentes disruptivos y los impactos asociados.
2. Identificacion de los recursos financieros necesarios para responder a un incidente disruptivo.
3. Capacidades de comunicación eficaces, tanto internas, como externas.
4. Capacidades para disponer de un espacio de trabajo alternativo con el fin de abordar la pérdida de instalaciones o la imposibilidad de acceso a estas.
5. Medidas para abordar la falta de disponibilidad del personal.
6. Métodos alternativos para mantener, corregir y sustituir los recursos con los que se llevan a cabo las actividades.
7. Capacidades para recuperar los activos de tecnologías de la información y comunicación (TIC). Incluidos los datos que se hayan perdido.
8. Medios alternativos para entregar los productos y prestar los servicios en caso de una interrupción de la cadena de suministro.

Entre las personas que determinen y seleccionen las estrategias de continuidad del negocio, deben haber personas que:

1. **Cuenten con una perspectiva panorámica de toda la organización.**
2. **Conozcan la estrategia de negocio actual y futura.**
3. **Tengan la autoridad para la toma de decisiones.**
4. **Conozcan profundamente los productos, servicios, procesos, actividades y recursos de la organización.**
5. **Estén familiarizados con los requisitos de toma de decisiones y desembolso de capital de la organización.**
6. **Comprendan los resultados del análisis de impacto en el negocio (BIA) y de la evaluación de riesgos (RIA) y entiendan el proceso de determinación y selección de las estrategias de continuidad del negocio.**

“Los responsables de determinar y seleccionar las estrategias, deben contar con el pleno respaldo de la alta dirección…”

En concreto, ¿Qué nos propone ISO 22331:2020?

Información y Datos

Indisponibilidad de la Información

ESTRATEGIA DE CORTO PLAZO

Replicación de datos

Proveedor de Servicio Externo

ESTRATEGIA DE LARGO PLAZO

Soluciones de réplica en línea (alta disponibilidad)

Externalización del CPD. Alianzas estratégicas.

Instalaciones

Indisponibilidad de Instalaciones

ESTRATEGIA DE CORTO PLAZO

Realocación en oficinas

Teletrabajo

ESTRATEGIA DE LARGO PLAZO

Establecer acuerdos con otra organización o contratar proveedores de servicios de recuperación

Inspeccionar, acondicionar e invertir en los espacios de trabajo remote seguro

Personas

Indisponibilidad de Personal

ESTRATEGIA DE CORTO PLAZO

Reasignación de funciones

Contratación de personal de apoyo

ESTRATEGIA DE LARGO PLAZO

Contratar personal temporal a través de agencias externas

Contactar a antiguos empleados de la empresa y contratar servicios específicos

Consideraciones finales

Resumen 1

ISO 2331:2020 nos invita a replantear nuestras estrategias de continuidad con una mirada de Largo Plazo.

Resumen 2

El Análisis de Impacto en el Negocio (BIA) y la evaluación de Riesgos (RIA), siguen siendo herramientas relevantes a la hora de definir una estrategia de continuidad.

Resumen 3

Las estrategias de continuidad de negocio no son infalibles, siempre deben ser probadas y mejoradas en el tiempo.

Resumen 4

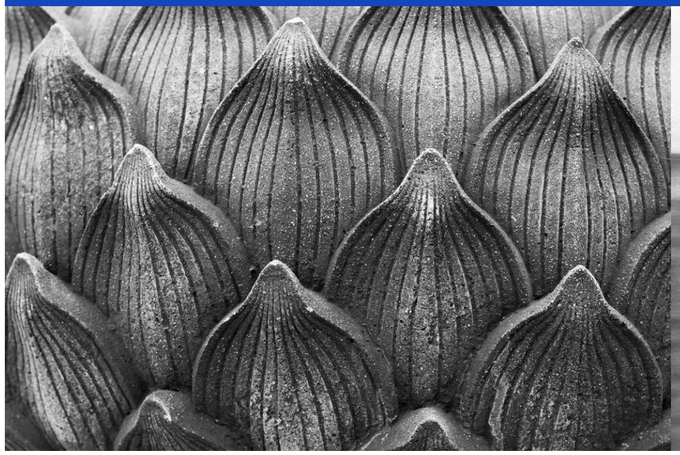
No hay una fórmula mágica para definir una estrategia adecuada, pero el conocimiento del negocio y de su entorno, permitirán seleccionar la estrategia más adecuada.

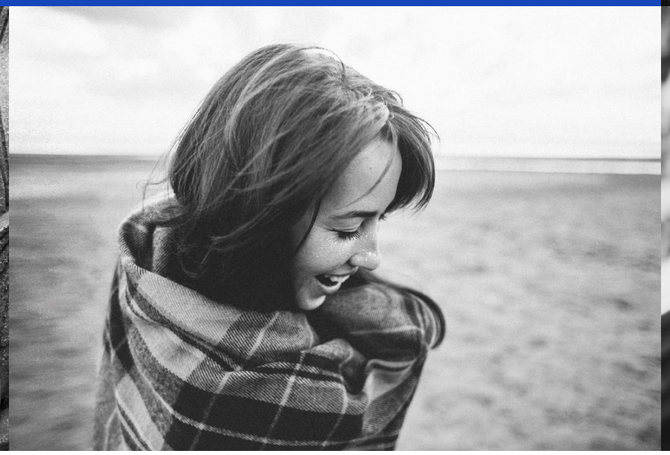
SOCHISI
DIGITAL SECURITY THINK TANK

ISO 22331:2020 nos invita a abrir la mente y pensar en estrategias de continuidad de negocio para el breve, corto y largo plazo.

La efectividad de cada estrategia la dará el tiempo, sin embargo...

“No hay peor estrategia de continuidad de negocio, que no contar con una estrategia de continuidad de negocio”

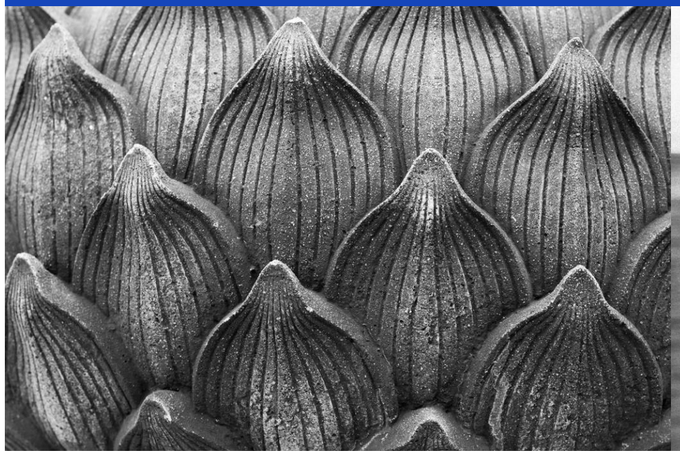


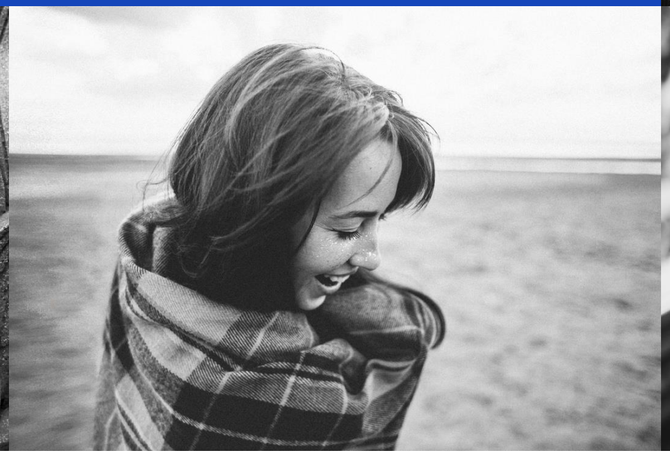


SOCHISI
DIGITAL SECURITY THINK TANK

¿Cuál es el límite para la definición de una estrategia de continuidad?

No hay límite...Hasta donde nuestra imaginación y creatividad lo permitan.





12 MARZO 2021

II CONGRESO DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD

“Muchas gracias”

SOCHISI
DIGITAL SECURITY THINK TANK

Speaker:
Cristian Maldonado Urrutia

Linkedin
www.linkedin.com/in/cmaldonadou

SOCHISI.CL/ENVIVO