CONTROL 17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DEL NEGOCIO

NORMA ISO/IEC 27001: 2013

OasisCom
Cloud Solutions

Tabla de contenido

OasisCom
Cloud Solutions

Controles de Continuidad del Negocio en la Norma ISO/IEC 27001:2013

Control A.17.1 Continuidad de seguridad de la información

- ✓ Control 1.17.1.1 **Planificación** de la continuidad de la seguridad de la información.
- ✓ Control 1.17.1.2 **Implementación** de la continuidad de la seguridad de la información.
- ✓ Control 1.17.1.3 **Verificación**, revisión y evaluación de la continuidad de la seguridad de la información.

Control A.17.2 Redundancias

- ✓ Control 1.17.2.1 Disponibilidad de instalaciones de procesamiento de información.

OasisCom
Cloud Solutions

Riesgos y Planes de Acción Seguridad de la Información

Riesgo

Falla en el servicio eléctrico.

Tiempo Estimado

1 – 3 días

Responsable

Gerencia Financiera

Plan de Acción

- ✓ Se debe validar con la administración del edificio la posibilidad del suministro eléctrico durante el tiempo que dure la emergencia.
- ✓ En caso de no disponer del suministro eléctrico por parte del edificio, se deberá alquilar un generador eléctrico de tal manera que el suministro sea constante y estable.

OasisCom Cloud Solutions

Riesgos y Planes de Acción Seguridad de la Información

Riesgo

Falla en el servicio de internet.

Tiempo Estimado

1 – 3 días

Responsable

Director de Infraestructura

Plan de Acción

- ✓ Identificar si el origen de la falla es interno o externo y ejecutar reparaciones cuando sea necesario.
- ✓ Disponer de servicio de internet móvil para mantener la operatividad de las áreas críticas de la organización.

OasisCom Cloud Solutions

Riesgos y Planes de Acción Seguridad de la Información

Riesgo

No disponibilidad de instalaciones físicas

Tiempo Estimado

30 – 90 días

Responsable

Gerencia General

Plan de Acción

- ✓ Evaluar la disponibilidad del lugar de operación de la organización y en caso de requerirse nuevas instalaciones físicas.
- ✓ Establecer el nuevo esquema de trabajo para las áreas críticas de la organización en pro de continuar con la prestación del servicio.
- ✓ Informar a las partes interesadas la ubicación de las instalaciones físicas o si se operara de forma virtual.

OasisCom Cloud Solutions

Riesgos y Planes de Acción Seguridad de la Información

Riesgo

Daño de activos tecnológicos utilizados en la operación (servidores, portátiles, firewall)

Tiempo Estimado

5 – 15 días

Responsable

Director de Infraestructura

Plan de Acción

- ✓ Identificar cantidad, características y tipos de activos tecnológicos necesarios, cuando el área afectada no sea critica para la organización se debe cubrir máximo el 20% de elementos tecnológicos.
- ✓ Evaluar criticidad y plan de acción según el documento *OR_SGSI_04_Matriz_de_Riesgos_del_SGSI*.
- ✓ Contactar los proveedores definidos en búsqueda de cotizaciones y/o negociaciones de los elementos requeridos.
- ✓ Adquirir los elementos tecnológicos requeridos, se puede utilizar esquema de compra o alquiler según la criticidad de las áreas afectadas.
- ✓ Instalación del software necesario para la continuidad de las labores.

OasisCom Cloud Solutions

Riesgos y Planes de Acción Seguridad de la Información

Riesgo

Daño en infraestructura de redes y comunicaciones

Tiempo Estimado

5 – 10 días

Responsable

Departamento de Infraestructura

Plan de Acción

- ✓ Identificar los elementos dañados requeridos para el funcionamiento de la red.
- ✓ Contactar los proveedores en búsqueda de cotizaciones y/o negociaciones de los elementos requeridos.
- ✓ Adquirir los elementos tecnológicos requeridos.
- ✓ Realizar la instalación y puesta en funcionamiento de la infraestructura de redes y/o comunicaciones.

OasisCom Cloud Solutions

Riesgos y Planes de Acción Seguridad de la Información

Riesgo

Pérdida de información confidencial

Tiempo Estimado

1 – 3 días

Responsable

Director de Infraestructura

Plan de Acción

- ✓ Identificar criticidad de la información perdida, por ejemplo, código fuente, contratos de clientes, avances de proyectos, etc.
- ✓ Verificar la existencia en copias de seguridad de la organización.
- ✓ Si la información existe se debe ejecutar el proceso de recuperación de copias de seguridad según lo establecido en el documento *PR_SGSI_03_Procedimientos_y_Politicas_Operacionales* ítem *Gestión de copias de seguridad*.

OasisCom
Cloud Solutions

Riesgos y Planes de Acción Seguridad de la Información

Riesgo

No disponibilidad de base de datos de producción

Tiempo Estimado

1 día

Responsable

Director de Infraestructura

Plan de Acción

- ✓ Cuando la base de datos alojada en la plataforma de *Microsoft Azure* presente fallas de funcionamiento se deberá realizar una restauración desde el ultimo punto de copia de seguridad existente y seguir lo establecido en el documento *PR_SGSI_03_Procedimientos_y_Politicas Operacionales* ítem *Gestión de copias de seguridad*.

OasisCom Cloud Solutions

Recomendaciones generales sobre los Planes de Acción de Seguridad de la Información

Cuando la emergencia así lo requiera se pueden utilizar **lugares de trabajo alternos** a la oficina principal de OasisCom.

OasisCom
Cloud Solutions

Recomendaciones generales sobre los Planes de Acción de Seguridad de la Información

Para las plataformas de Microsoft Azure y Firewall (Fortigate) se realizarán pruebas de restablecimiento en **escenarios controlados** similares a los de producción y se deben proteger con la misma criticidad que los ambientes reales.

OasisCom
Cloud Solutions

Recomendaciones generales sobre los Planes de Acción de Seguridad de la Información

Cuando el Director de Infraestructura no pudiese cumplir sus funciones de administración y gestión de plataformas, el **Gestor de Soporte Nivel 1** deberá respaldar la operación y velar por la Seguridad de la Información acorde a las políticas definidas ambientes reales.

OasisCom
Cloud Solutions

Protección del código fuente

Para controlar el código fuente de nuestro software **OasisCom** y la base de conocimiento, se utiliza la plataforma ***Microsoft Team Foundation,*** la cual nos proporciona la documentación en cualquier momento.

Esta plataforma sigue los esquemas de protección, copias de seguridad y restauración definidos en el documento *PR_SGSI_03_Procedimientos_y_Politicas_Operacionales* ítems *Gestión de copias de seguridad* y *Procedimiento de restablecimiento de código fuente (TFS).*

OasisCom
Cloud Solutions

Cronograma de ejecución de pruebas de restablecimiento de plataformas

Plataforma	Descripción	Mes de ejecución	Responsable
Redes y Firewall	Pruebas de restablecimiento de controles de acceso a la red a través del dispositivo Firewall.	Octubre	Director de Infraestructura
Microsoft Azure (Bases de datos)	Pruebas de restablecimiento de acceso a base de datos de producción. Se podrán utilizar escenarios controlados	Noviembre	Director de Infraestructura
Microsoft Azure (Aplicación OasisCom)	Pruebas de restablecimiento de aplicación OasisCom de producción. Se podrán utilizar escenarios controlados.	Diciembre	Director de Infraestructura
Microsoft Team Foundation (Código Fuente)	Pruebas de restablecimiento de acceso a archivos de código fuente.	Diciembre	Director de Infraestructura

OasisCom Cloud Solutions


OasisCom
Cloud Solutions
You
Tube