PLAN DE GESTION DE RIESGOS CORPORATIVOS

SISTEMAS DE GESTION DE LA SEGURIDAD DE LA INFORMACIÓN

ING. JOHN ROBERTH CORREA

INTEGRANTES DEL GRUPO:

LUIS FELIPE VELASCO TAO

JUAN DAVID GONZALEZ DIMATÉ

UNIVERSIDAD DE SAN BUENAVENTURA

FACULTAD DE INGENIERÍA

INGENIERÍA DE SISTEMAS

BOGOTÁ

29 DE ABRIL

2021-1

Contenido

Generalidades

La siguiente política define los estándares y protocolos a seguir para preservar adecuadamente todo componente de la infraestructura de la organización teniendo como base la norma ISO 17799. Dentro de dicha infraestructura se contempla todo equipo, instrumento o lugar en uso por la organización y para el cumplimiento de sus objetivos, así como sus funciones básicas. Esta infraestructura se compone de:

- Ordenadores.
- Escritorios.
- Puestos de trabajo (cubículos, oficinas, entre otros).
- Instalaciones.
- Servidores.
- Equipos de red.
- Mantenimiento de equipos.
- Personal.

Objetivos

El objetivo de este plan es diseñar un plan de control para mitigar los riesgos relacionados a la seguridad física y ambiental de la organización, en donde pueden comprometerse tanto los equipos físicos en uso de la organización, como los elementos abstractos en posesión de ella, tales como la información de clientes y empleados. Además, debe contemplarse que estos riesgos pueden influir en mayor o menor medida a la seguridad del personal. Estos riesgos pueden incluir el acceso no regulado a las instalaciones de la organización o a daños que puedan afectar negativamente a la integridad física de los empleados o los directivos, como incendios eléctricos o explosiones por cortocircuitos en los equipos físicos.

Riesgos y afectaciones

Teniendo en cuenta el objetivo del plan de gestión de riesgos corporativos en curso, los riesgos potenciales identificados están relacionados fuertemente con los aspectos que involucran:

- Afectaciones en los ordenadores y derivados.
- Afectaciones en los servidores y derivados.
- Afectaciones en la estructura de las instalaciones y derivados.
- Afectaciones en el sistema de acceso de la organización y derivados.
- Afectaciones en la integridad física de los empleados y derivados.

Con base en ellos, se presentarán los riesgos que pueden afectar a la organización desde estos aspectos, teniendo en cuenta la rúbrica estándar para la clasificación de riesgos.

Probabilidad	Impacto				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

B= Zona de riesgo baja: Se asume el riesgo.
M= Zona de riesgo moderada: Asumir el riesgo Reducir el riesgo.
A= Zona de riesgo alto: Reducir el riesgo, Evitar, Compartir o Transferir
E= Zona de riesgo Extremo: Reducir el riesgo, Evitar, Compartir o Transferir.

Soft-easy

Riesgos identificados

Riesgo		Calificación		Evaluación
Tipo	Descripción	Probablilidad	Impacto	Zona de riesgo
Operativo	Fallo de equipos	3	3	Alto
Tecnológico	Rendimiento deficiente	3	2	Moderado
Tecnológico	Corrupción del ordenador	1	3	Moderado
Tecnológico	Colapso del sistema	3	3	Alto
Tecnológico	Desconexión del servicio	4	3	Alto
Operativo	Pérdida total o parcial del servicio	3	3	Alto
Operativo	Pérdida de comunicación con los servidores	3	4	Extremo
Tecnológico	Daño en los servidores	3	4	Extremo
Tecnológico	Robo de los servidores	1	5	Alto
Operativo	Apagones	1	2	Bajo
Operativo	Cortes de red	1	2	Bajo
Operativo	Acceso no autorizado a las instalaciones	3	3	Alto
Operativo	Acceso no autorizado a zonas restringidas	1	5	Alto
Tecnológico	Acceso no autorizado al sistema informático	2	4	Alto
Operativo	Accidentes laborales por daño en las instalaciones	1	5	Alto
Tecnológico	Accidentes laborales por daño en los equipos	2	4	Alto

Plan de acción

Es responsabilidad de la organización proveer estándares para la preservación del buen estado tanto de las instalaciones como de los equipos en uso, con el objetivo de prevenir cualquier riesgo o accidente que pueda ocurrir y, por ende, que pueda afectar a la salud del personal o a los objetivos y/o funciones de la organización. Es por esto por lo que surge la necesidad de que el personal empleado por la organización sea adecuadamente capacitado.

La capacitación debe incluir pautas de uso de los equipos, niveles de acceso dentro de las instalaciones, pautas para el personal autorizado, lineamientos de comportamiento y posibles riesgos, junto con sus causas. Además, esta capacitación debe incluir (siempre variando con respecto a las funciones del personal) los siguientes lineamientos:

- Uso de equipos.
- Número de dispositivos conectados en un mismo lugar.
- Protección de equipos.
- Accesos autorizados.
- Normas de comportamiento.
- Control de equipos y permisos.

El acceso a las diferentes zonas de las instalaciones está determinado por el rol y las funciones que deban cumplir los empleados, los cuales serán distinguidos por una tarjeta de identificación que les será provista al momento de su ingreso formal a la organización.

Responsables

La responsabilidad con respecto a la organización está determinada en tres clases:

Responsabilidad administrativa.

Corresponde al funcionamiento gerencial de la organización, lo que incluye a las decisiones tomadas con respecto a la misión, objetivos, elementos necesarios para su cumplimiento y el personal requerido para ello. Esta responsabilidad recae en:

- Alta gerencia: La entidad de mayor nivel en la organización (suele referirse a la presidencia, las directivas y los ejecutivos) cuya función principal es tomar las decisiones necesarias para el funcionamiento de la compañía.

Responsabilidad empresarial.

Corresponde al funcionamiento de la organización con respecto a su misión y/o sus objetivos. Esta responsabilidad comprende al personal con los conocimientos técnicos necesarios para el cumplimiento de los objetivos de Soft-easy como empresa de desarrollo de software. Esta responsabilidad recae en:

- Desarrolladores: Encargados de mantener en buen estado sus puestos de trabajo y de proporcionar un uso adecuado a los equipos que utilicen para el cumplimiento de su labor en la empresa.
- Mantenimiento: Encargados de mantener los equipos de red y servidores en buen estado, además de proporcionar una revisión periódica de los equipos utilizados por el personal.

Responsabilidad sobre las instalaciones

Corresponde al acceso del personal en las instalaciones y a su comportamiento dentro de las mismas. Cabe resaltar que cada miembro del personal (desde la Alta

gerencia hasta los empleados particulares) tienen el deber de cuidar en la medida de lo posible las instalaciones, manteniéndolas limpias y evitando cualquier tipo de interacción que puedan afectar su integridad (golpes, humedad, desgaste, etc.).

Los responsables del acceso a las instalaciones son:

- Personal de seguridad: Encargados de supervisar la entrada del personal a las instalaciones y cualquier movimiento sospechoso y/o no autorizado dentro de las mismas.

Controles de mitigación de riesgos

Para todo control que se deba aplicar, siempre hay que evaluar su efectividad al momento de tratar el riesgo, por lo que se hace necesario aplicar una valoración de controles. Esta valoración está determinada por:

Descripción del control	Criterios para la evaluación	Evaluación		Observaciones
		Sí	No	
Describa el control determinado para el riesgo identificado	¿El control previene la materialización del riesgo (afecta probabilidad) ¿El control permite enfrentar la situación en caso de materialización (afecta impacto)?	N/A	N/A	Este criterio no puntúa, es relevante determinar si el control es preventivo (probabilidad) o si es correctivo que permite enfrentar el evento una vez materializado (impacto), con el fin de establecer el desplazamiento en la matriz de evaluación de riesgos.
	¿Existen manuales, instructivos o procedimientos para el manejo del control?	15	0	
	¿Está(n) definido(s) el(los) responsable(s) de la ejecución del control y del seguimiento?	5	0	
	¿El control es automático? (Sistemas o Software que permiten incluir contraseñas de acceso, o con controles de seguimiento a aprobaciones o ejecuciones que se realizan a través de éste, generación de reportes o indicadores, sistemas de seguridad con scanner, sistemas de grabación, entre otros).	15	0	
Describa el control determinado para el riesgo identificado	¿El control es manual? (Políticas de operación aplicables, autorizaciones a través de firmas o confirmaciones vía correo electrónico, archivos físicos, consecutivos, listas de chequeo, controles de seguridad con personal especializado, entre otros)	10	0	
	¿La frecuencia de ejecución del control y seguimiento es adecuada?	15	0	
	¿Se cuenta con evidencias de la ejecución y seguimiento del control?	10	0	
	¿En el tiempo que lleva la herramienta ha demostrado ser efectiva?	30	0	
	TOTAL	100	0	

Tabla para evaluación de riesgos según valoración de controles.

RANGOS DE CLASIFICACIÓN DE LOS CONTROLES	DEPENDIENDO SI EL CONTROL AFECTA PROBABILIDAD O IMPACTO SE DESPLAZA EN LA MATRIZ DE CALIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS.	
	CUADRANTE A DISMINUIR EN LA PROBABILIDAD	CUADRANTE A DISMINUIR EN EL IMPACTO
ENTRE 0-50	0	0
ENTRE 51-75	1	1
ENTRE 76-100	2	2

Adaptando este formato a este plan, y teniendo como base actividades anteriores, la rúbrica a utilizar será implementada de la siguiente manera:

Parámetros	Criterios	Evaluación		Tipo de control (Probabilidad o impacto)	Puntaje	Puntaje final
		Si	No			
Herramientas para ejercer el control	¿Posee una herramienta para ejercer el control?			Probabilidad	15	85
	¿Existen manuales, instructivos o procedimientos para el manejo de la herramienta?				15	
	¿El tiempo que lleva la herramienta ha demostrado ser efectiva?				30	
eguimiento al contro	¿Están definidos los responsables de la ejecución del control y del seguimiento?				0	
	¿La frecuencia de ejecución del control y del seguimiento es adecuada?				25	

Seguridad física y del entorno

Los puestos de trabajo de los desarrolladores estarán dispuestos en un espacio ventilado y con iluminación. El espacio debe incluir una oficina dispuesta para el supervisor y debe albergar un máximo de 5 puestos de trabajo. La entrada del espacio en el que estén dispuestos debe incluir un lector de tarjetas que le permita el acceso a los desarrolladores y al personal de mantenimiento con el nivel de acceso adecuado.

Los servidores deben estar alejados de los baños, cocinas y cualquier lugar que tenga un flujo de agua o gas constante, debe estar ventilado y asegurado contra impactos externos (como objetos). La sala de los servidores debe tener un lector de tarjetas y tres guardias de seguridad con turnos rotatorios.

El personal de desarrollo debe especificar claramente sus necesidades de desarrollo, con el fin de ajustar adecuadamente los componentes de los equipos. Esto con el propósito de evitar algún tipo de sobrecarga en los ordenadores que pueda causar algún tipo de malfuncionamiento o cortocircuito. Estas especificaciones deberán realizarse una semana antes de iniciar el desarrollo de un proyecto mediante una carta formal a la gerencia.

La gerencia tiene el deber de revisar la carta de especificaciones y decidir si aprobarla, rechazarla o modificarla, con el fin de gestionar adecuadamente el presupuesto disponible. Luego de esto deben solicitar los componentes necesarios para el ajuste adecuado de los equipos. Finalmente, la gerencia debe dar la orden de modificación de los equipos al personal correspondiente.

El personal de mantenimiento con el nivel de acceso correspondiente tiene el deber de ajustar los equipos de trabajo conforme a lo establecido en la orden de gerencia.

CR01						
Parámetros	Criterios	Evaluación		Tipo de control (Probabilidad o impacto)	Puntaje	Puntaje final
		Si	No			
Herramientas para ejercer el control	¿Posee una herramienta para ejercer el control?			Probabilidad	15	70
	¿Existen manuales, instructivos o procedimientos para el manejo de la herramienta?				15	
	¿El tiempo que lleva la herramienta ha demostrado ser efectiva?				0	
Seguimiento al control	¿Están definidos los responsables de la ejecución del control y del seguimiento?				15	
	¿La frecuencia de ejecución del control y del seguimiento es adecuada?				25	

Control de acceso

El acceso a las oficinas de desarrollo será resguardado por un sistema que identifique a los miembros que hagan parte de la organización en distintos roles, mediante un carné de identificación. Además, aquellos empleados que estén identificados como personal de mantenimiento deberán ser categorizados con respecto a su área correspondiente en niveles de acceso. Estos niveles de acceso serán divididos en los números 1,2 y 3, siendo el número 1 asignado a los encargados del área de mantenimiento general (limpieza y mantenimiento general de las instalaciones), el número 2 asignado a los encargados de mantenimiento de los equipos de desarrollo y el número 3 asignado a los encargados del mantenimiento de los servidores.

CR02						
Parámetros	Criterios	Evaluación		Tipo de control (Probabilidad o impacto)	Puntaje	Puntaje final
		Si	No			
Herramientas para ejercer el control	¿Posee una herramienta para ejercer el control?			Impacto	15	100
	¿Existen manuales, instructivos o procedimientos para el manejo de la herramienta?				15	
	¿El tiempo que lleva la herramienta ha demostrado ser efectiva?				30	
Seguimiento al control	¿Están definidos los responsables de la ejecución del control y del seguimiento?				15	
	¿La frecuencia de ejecución del control y del seguimiento es adecuada?				25	

Uso de equipos

Cada miembro del personal en general debe seguir los siguientes lineamientos:

- Utilizar su equipo de trabajo dentro de los horarios laborales establecidos.
- No instalar programas ni aplicaciones sin la debida revisión de su fuente o sin el consentimiento informado del personal de mantenimiento.
- No manipular los componentes físicos de los equipos (procesador, memoria RAM, etc.) sin el consentimiento del personal de mantenimiento.
- Mantener su equipo de trabajo en lugares en donde no pueda ser golpeado por accidente, o frecuentemente (por ejemplo, cerca de sus pies).
- No intentar acceder de ninguna manera a la BIOS de los ordenadores, ni modificar cualquier característica dentro de ella.
- De surgir la necesidad de realizar algún tipo de modificación en los ordenadores (aumentar su capacidad o rendimiento), primero debe informarse a la alta gerencia sobre estos cambios, o en su defecto al personal de mantenimiento.

Con respecto al uso particular de los equipos, dependiendo de su rol dentro de la organización deberá seguir un número de pautas adicionales. Para los desarrolladores:

- Si surge la necesidad de modificar un componente de un equipo, deberá realizar una solicitud formal a la alta gerencia mediante una carta. Esta carta

deberá incluir: Tipo, motivo y necesidad de la solicitud. Además, debe informar con antelación al personal de mantenimiento sobre la realización de la solicitud.

- Si surge la necesidad de utilizar los equipos más allá del tiempo establecido (debido a la falta de tiempo para la culminación de un proyecto o el retraso del desarrollo por motivos de fuerza mayor), deberá realizar una solicitud formal a la alta gerencia para su aprobación. Esta solicitud debe incluir: Tipo, motivo y necesidad de la solicitud, junto con la fecha en la que va a realizar este tiempo adicional y la duración de este. La solicitud debe realizarse con un mínimo de 3 días hábiles de antelación.
- Si surge la necesidad de alterar algún componente de la BIOS, el desarrollador deberá informar al personal de mantenimiento capacitado, el cual estará en la autoridad de decidir si dicha alteración es estrictamente necesaria o no.
- Evitar sobrecargar la capacidad del equipo trabajando con programas con un consumo de recursos altos simultáneamente.

Para el personal de mantenimiento:

- Debe asegurarse que cualquier equipo físico esté ubicado en zonas ajenas a cualquier influencia ambiental que pueda provocar fallos en ellos (como zonas húmedas, calurosas, con corriente inestable, etc.).
- Para cualquier modificación en los equipos indicada en una solicitud aprobada por la alta gerencia, debe dejar un registro indicando: Fecha y hora de la modificación, tipo de modificación, y herramientas y componentes utilizados para ella.
- En el caso de realizar cambios a la BIOS, deberá realizar un informe detallado sobre los cambios realizados. Este informe debe incluir: Fecha y hora de la modificación, tipo de modificación realizada y procedimiento detallado de ella.
- Debe realizar una revisión diaria a los servidores y a los equipos de red para asegurarse de que cumplan con los lineamientos de ubicación y de acceso adecuados.

CR03						
Parámetros	Criterios	Evaluación		Tipo de control (Probabilidad o impacto)	Puntaje	Puntaje final
		Si	No			
Herramientas para ejercer el control	¿Posee una herramienta para ejercer el control?			Impacto	15	100
	¿Existen manuales, instructivos o procedimientos para el manejo de la herramienta?				15	
	¿El tiempo que lleva la herramienta ha demostrado ser efectiva?				30	
Seguimiento al control	¿Están definidos los responsables de la ejecución del control y del seguimiento?				15	
	¿La frecuencia de ejecución del control y del seguimiento es adecuada?				25	

Seguridad del personal

Cada miembro del personal deberá seguir los siguientes lineamientos:

- Mantenerse alejado de las zonas que su nivel de acceso restringe.
- Mantener sus manos limpias y secas al momento de manipular algún tipo de dispositivo electrónico o al momento de utilizar su equipo de trabajo.
- Mantener una distancia prudente entre las tomas de corriente y su persona.
- Evitar ocupar todas las tomas de corriente con distintos dispositivos (cargadores, baterías, etc.).

Con base en el rol de cada miembro del personal, deberán seguir lineamientos adicionales. Para el desarrollador:

- Evitar realizar modificaciones en los equipos o puestos de trabajo sin el permiso, supervisión o equipamiento adecuado (reubicaciones o adición de componentes a la CPU).

Para el personal de mantenimiento:

- Al momento de realizar algún tipo de modificación a los componentes físicos de los equipos, asegurarse de que no estén recibiendo ningún tipo de corriente.
- Asegurarse de utilizar equipo con propiedades aislantes al momento de tratar con componentes electrónicos.

- En caso de haber algún tipo de afectación en la estructura de las instalaciones debido al peso de algún componente (servidores y/o puestos de trabajo), tiene la autoridad de reubicar dichos componentes a un lugar más conveniente, siguiendo los lineamientos de ubicación establecidos por la gerencia.
- Debe contar con el adecuado equipo de seguridad dependiendo de su nivel de acceso (Botas y guantes aislantes para cualquier nivel de acceso, lentes para el nivel 2, lentes, chaleco y casco para el nivel 3).

CR04						
Parámetros	Criterios	Evaluación		Tipo de control (Probabilidad o impacto)	Puntaje	Puntaje final
		Si	No			
Herramientas para ejercer el control	¿Posee una herramienta para ejercer el control?			Impacto	0	85
	¿Existen manuales, instructivos o procedimientos para el manejo de la herramienta?				15	
	¿El tiempo que lleva la herramienta ha demostrado ser efectiva?				30	
Seguimiento al control	¿Están definidos los responsables de la ejecución del control y del seguimiento?				15	
	¿La frecuencia de ejecución del control y del seguimiento es adecuada?				25	

Cumplimiento

Con base en los controles aplicados, se debe realizar una matriz de riesgo que evidencie la efectividad de los controles y muestre el resultado de haberlos aplicado a los riesgos correspondientes. Esta matriz se encuentra en el Anexo A: Matriz de riesgos corporativos.