GUÍA PARA LA GESTIÓN DE
RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

MINISTERIO DE TELECOMUNICACIONES
Y DE LA SOCIEDAD DE LA INFORMACIÓN

Lenín
Toda una Vida
EL GOBIERNO DE TODOS

Contenido

INTRODUCCIÓN

La revolución digital ha generado que las organizaciones a nivel mundial tomen mayor atención a la información, actor principal de este proceso de cambio. Este proceso ha permitido establecer nuevas alianzas y acortar distancias entre naciones, donde el internet cumple un papel fundamental en la comunicación.

En términos de gestión de riesgos de seguridad de la información, el activo a proteger es la información, tanto de información digital, contenida en los sistemas de información como aquella contenida en cualquier otro medio como por ejemplo el papel. Debemos tener presente que la gestión debe ocuparse de todo el ciclo de vida de la información.

Es necesario un enfoque sistemático para la gestión del riesgo en la seguridad de la información para identificar las necesidades de la organización con respecto a los requisitos de seguridad de la información y para crear un eficaz sistema de gestión de la seguridad de la información – SGSI -.

Este enfoque debe ser adecuado para el entorno de la institución y, en particular, debería cumplir los lineamientos de toda la gestión del riesgo de la institución.

Los esfuerzos de seguridad deben abordar los riesgos de una manera eficaz y oportuna donde y cuando sean necesarios. La gestión del riesgo de la seguridad de la información debe ser una parte integral de todas las actividades de la gestión de la seguridad de la información y se deben aplicar tanto a la implementación como al funcionamiento continuo de un SGSI.

La gestión del riesgo de la seguridad de la información debe ser un proceso continuo. Tal proceso debe establecer el contexto, evaluar los riesgos, tratar los riesgos utilizando un plan de tratamiento para implementar las recomendaciones y decisiones.

"La gestión del riesgo analiza lo que puede suceder y cuáles pueden ser las posibles consecuencias, antes de decidir lo que se debe hacer y cuando hacerlo, con el fin de reducir el riesgo hasta un nivel aceptable".

CONCEPTOS BÁSICOS

La información es el activo principal pero también debemos considerar: infraestructura informática, equipos auxiliares, redes de comunicaciones, instalaciones y personas.

Cuando hablamos de seguridad de la información hablamos de protegerla de riesgos que puedan afectar a una o varias de sus tres principales propiedades:

Confidencialidad: La información solo tiene que ser accesible o divulgada a aquellos que están autorizados.

Integridad: La información debe permanecer correcta (integridad de datos) y como el emisor la originó (integridad de fuente) sin manipulaciones por terceros.

Disponibilidad: La información debe estar siempre accesible para aquellos que estén autorizados.

Figura No.1 PRINCIPIOS DE LA S.I.,
Fuente: https://infosegur.wordpress.com/tag/disponibilidad/

Para facilitar el proceso de análisis y valoración de los riesgos es importante entender algunos conceptos básicos:

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Amenaza: causa potencial de un incidente no deseado, que puede resultar en un daño a un sistema, persona u organización.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

Impacto: es la consecuencia de la materialización de una amenaza sobre un activo. El costo para la institución de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros (ejem.: pérdida de reputación, implicaciones legales, entre otros).

Riesgo inherente: Es el riesgo existente y propio de cada actividad, sin la ejecución de ningún control.

Riesgo **residual**: El riesgo que permanece tras el tratamiento del riesgo.

PROCESO PARA LA GESTIÓN DEL RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN

El proceso de gestión del riesgo de la seguridad de la información puede ser iterativo para las actividades de valoración del riesgo y/o de tratamiento del riesgo. Un enfoque iterativo para realizar la valoración del riesgo puede incrementar la profundidad y el detalle de la valoración en cada iteración. El enfoque iterativo suministra un buen equilibrio entre la reducción del tiempo y el esfuerzo requerido para identificar los controles, incluso garantizando que los riesgos de impacto alto se valoren de manera correcta.

Actividades para la gestión del riesgo de la seguridad de la información:

- Establecimiento del contexto
- Valoración del riesgo
- Tratamiento del riesgo
- Aceptación del riesgo
- Comunicación del riesgo
- Monitoreo y revisión del riesgo

Pasos de las actividades del proceso de gestión del riesgo:

PROCESO PARA LA GESTIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN	
ACTIVIDADES	**PASO**
Establecimiento del contexto	**1** *Consideraciones Generales - Levantamiento de información inicial* **2** *Establecer criterios básicos para la Gestión del Riesgo* **3** *Definir alcance y límites de la Gestión del Riesgo* **4** *Establecer una organización para la operación del SGRSI*
Valoración del Riesgo	**5** *Identificar Activos de Información* **6** *Identificar las amenazas y las vulnerabilidades* **7** *Identificar los controles existentes* **8** *Identificar consecuencias* **9** *Valorar las consecuencias* **10** *Valorar los incidentes* **11** *Determinar el nivel de estimación del riesgo* **12** *Evaluar el riesgo*
Tratamiento del Riesgo	**13** *Seleccionar controles*
Aceptación del Riesgo	**14** *Aceptar el riesgo*
Comunicación del Riesgo	**15** *Comunicar el riesgo*
Monitoreo y Revisión del Riesgo	**16** *Monitorear y revisar los riesgos*

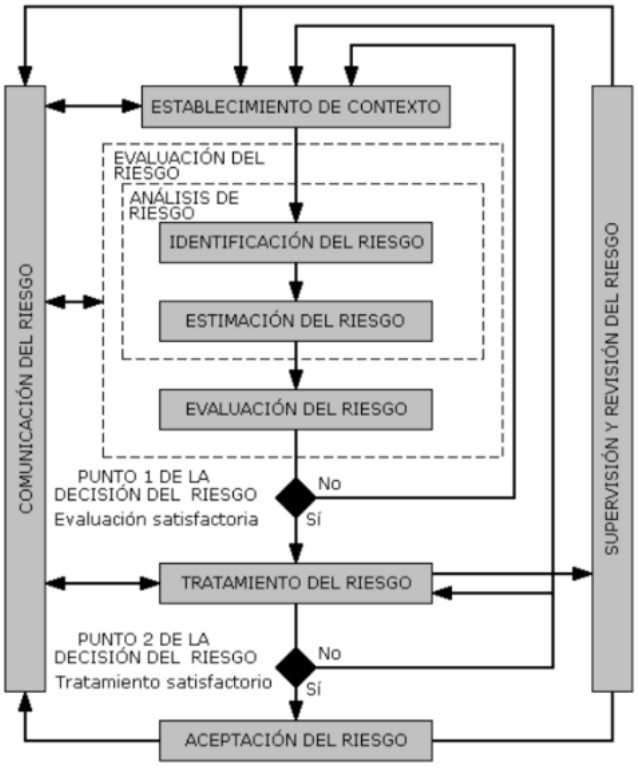

Figura No. 2 PROCESO DE GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN, Fuente: ISO27005

ESTABLECIMIENTO DEL CONTEXTO

Consideraciones generales

"Se debe establecer el contexto para la gestión del riesgo de la seguridad de la información, lo cual implica establecer los criterios básicos que son necesarios para la gestión del riesgo de la seguridad de la información: definir el alcance y los límites, establecer una organización adecuada que opere la gestión del riesgo de la seguridad de la información".

CRITERIOS BÁSICOS

Dependiendo del alcance y los objetivos de la gestión del riesgo, se pueden aplicar diferentes enfoques. El enfoque también podría ser diferente para cada iteración.

Es aconsejable seleccionar o desarrollar un enfoque adecuado para la gestión del riesgo que aborde los criterios básicos tales como: criterios de evaluación del riesgo, criterios de impacto, criterios de aceptación del riesgo, entre otros.

Criterios de identificación del riesgo

Es recomendable considerar los activos de información con el valor de impacto alto para el proceso de evaluación del riesgo.

Criterios de evaluación del riesgo

Es recomendable desarrollar criterios para la evaluación del riesgo con el fin de determinar el riesgo de la seguridad de la información de la institución.

Criterios de impacto

Es recomendable desarrollar criterios de impacto del riesgo y especificarlos en términos del grado de daño o de los costos para la organización, causados por un evento de seguridad de la información.

Criterios de la aceptación del riesgo

Es recomendable desarrollar y especificar criterios de aceptación del riesgo. Estos criterios dependen con frecuencia de las políticas, metas, objetivos de la institución y de las partes interesadas.

Las instituciones pueden definir sus propias escalas para los niveles de aceptación del riesgo.

Alcance y límites

Es necesario definir el alcance del proceso de gestión del riesgo de la seguridad de la información, con el fin de garantizar que todos los activos relevantes se toman en consideración en la valoración del riesgo. Además, es necesario identificar los límites para abordar aquellos riesgos que se pueden presentar al establecer estos límites.

Los ejemplos del alcance de la gestión del riesgo pueden ser una aplicación de tecnología de la información, infraestructura de tecnología de la información, un proceso del negocio o una parte definida de la institución

"El alcance y los límites de la gestión del riesgo de la seguridad de la información se relacionan con el alcance y los límites del Esquema Gubernamental de Seguridad de la información – EGSI -"

Organización para la gestión del riesgo de la seguridad de la información

Se recomienda establecer y mantener la organización y las responsabilidades en el proceso de gestión del riesgo y la seguridad de la información definidas en el acuerdo ministerial.

Esta organización para la gestión del riesgo, debería ser aprobada por la máxima autoridad de cada institución.

VALORACIÓN DEL RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN

"Los riesgos se deberían identificar, describir cuantitativa o cualitativamente y priorizar frente a los criterios de evaluación del riesgo y los objetivos relevantes para la institución"

Un riesgo es una combinación de las consecuencias que se presentarían después de la ocurrencia de un evento indeseado y de su probabilidad de ocurrencia. La valoración del riesgo cuantifica o describe cualitativamente el riesgo y permite a los propietarios de los activos priorizar los riesgos de acuerdo con su gravedad percibida u otros criterios establecidos.

"En este proceso se obtiene toda la información necesaria para conocer, valorar y priorizar los riesgos"

La valoración del riesgo consta de las siguientes actividades:

- Análisis del riesgo
  - Identificación del riesgo
  - Estimación del riesgo
- Evaluación del riesgo

ANÁLISIS DEL RIESGO

Identificación del riesgo

Consiste en determinar qué puede provocar pérdidas a la institución. La identificación del riesgo consta de las siguientes actividades:

- Identificación de los activos
- Identificación de las amenazas
- Identificación de vulnerabilidades
- Identificación de la existencia de controles.

Identificación de los activos

Un activo es todo aquello que tiene valor para la organización y que, por lo tanto, requiere de protección. Para la identificación de los activos se recomienda tener en cuenta que el sistema de información consta de más elementos que sólo hardware y software.

Se debería identificar al propietario de cada activo, para asignarle la responsabilidad y rendición de cuentas sobre éste. El propietario del activo puede no tener derechos de propiedad sobre el activo, pero tiene la responsabilidad de su producción, desarrollo, mantenimiento, uso y seguridad, según corresponda. El propietario del activo con frecuencia es la persona más idónea para determinar el valor que el activo tiene para la organización

"La identificación de los activos es un punto clave para la identificación de las amenazas, vulnerabilidades, y determinar el nivel de riesgo o exposición de los activos y la selección de controles para mitigarlos"

De este proceso se genera una lista de los activos que van a estar sometidos a gestión del riesgo, y una lista de los procesos del negocio relacionados con los activos y su importancia.

Para realizar la valoración de los activos, es necesario que la institución identifique primero sus activos (con un grado adecuado de detalles). De manera general se pueden diferenciar dos clases de activos:

Los activos primarios:

- Actividades y procesos del negocio.
- Información.

Los activos de soporte (de los cuales dependen los elementos primarios del alcance) de todos los tipos:

- Hardware.
- Software.
- Redes.
- Personal.
- Ubicación.
- Estructura de la organización.

Ejemplo de identificación de activos:

IDENTIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN						
Nro. Activo	**Proceso Macro**	**Subproceso**	**Tipo de Activo**	**Nombre de Activo**	**Descripción del activo**	**Ubicación**
A1	**Apoyo de Tecnologías de la Información y Comunicaciones**	**Infraestructura**	**Hardware**	Controladora Wireless, puntos de acceso	puntos de acceso inalámbrico en toda la institución	Data Center
A2			**Hardware**	Firewall Fortigate	Control de acceso y permisos de seguridad perimetral para la red institucional	Data Center
A3		**Redes y comunicaciones**	**Redes**	Switch Core Cisco 4700	Procesamiento de trafico de red para distribución en la red interna e Internet	Data Center
A4			**Redes**	Switchs de Acceso Cisco 2960	Procesamiento de trafico de red de acceso en cada piso del edificio	Data Center
A5		**Aplicaciones informáticas**	**Software**	Antivirus Institucional	Software de seguridad end point	Data Center
A6			**Software**	Servicio de correo Exchange	Información de buzones de correo electrónico institucional	Data Center
A7		**Instalaciones**	**Localidad**	Datacenter	Centro de Datos Institucional	Edificio Matriz
A8		**Talento Humano**	**Personal**	Personal de soporte	Funcionarios de Soporte Técnico Nivel 1 - Institucional	Edificio Matriz
A9			**Personal**	Personal de desarrollo de sistemas	Personal técnico que desarrolla aplicaciones o automatiza procesos	Edificio Matriz

Valoración de los activos / Ponderación de la criticidad de activos.

La ponderación de activos es una etapa en la que participan las unidades del negocio involucradas con el fin de determinar en términos cualitativos la criticidad de los distintos activos.

Esta ponderación fue realizada en términos de “alto, medio o bajo” donde se asigna un valor cuantitativo a cada valor cualitativo
A continuación, se presentan las referencias para la valoración del impacto en los activos de la información.

Valoración del impacto en términos de la perdida de la confidencialidad:

CONFIDENCIALIDAD	CRITERIO
Alto (3)	La divulgación no autorizada de la información tiene un efecto crítico para la institución Ej. Divulgación de información confidencial o sensible.
Medio (2)	La divulgación no autorizada de la información tiene un efecto limitado para la institución Ej. Divulgación de información de uso interno
Bajo (1)	La divulgación de la información no tiene ningún efecto para la institución Ej. Divulgación de información pública.

Valoración del impacto en términos de la perdida de la integridad:

INTEGRIDAD	CRITERIO
Alto (3)	La destrucción o modificación no autorizada de la información tiene un efecto severo para la institución
Medio (2)	La destrucción o modificación no autorizada de la información tiene un efecto considerable para la institución
Bajo (1)	La destrucción o modificación de la información tiene un efecto leve para la institución

Valoración del impacto en términos de la pérdida de la disponibilidad:

DISPONIBILIDAD	CRITERIO
Alto (3)	La interrupción al acceso de la información o los sistemas tienen un efecto severo para la institución
Medio (2)	La interrupción al acceso de la información o los sistemas tienen un efecto considerable para la institución
Bajo (1)	interrupción al acceso de la información o los sistemas tienen un efecto mínimo para la institución

Con referencia a las tablas mencionadas, la valoración se la realiza respecto a la confidencialidad, integridad y disponibilidad ya que estas son las dimensiones en que se basa la seguridad de la información.

VALORACIÓN DE LOS ACTIVOS DE INFORMACIÓN							
Nro. Activo	**Nombre de Activo**	**Tipo de soporte**	**Ubicación**	**Valoración de Impacto (pérdida)** **C: Confidencialidad** **I: Integridad** **D: Disponibilidad**			
				C	**I**	**D**	**VA**
A1	Controladora Wireless, puntos de acceso	Físico y Lógico	Centro de Datos	1	1	2	1,33
A2	Red de datos	Físico	Edificio Institucional	1	1	3	1,67
A3	Firewall Fortigate	Físico y Lógico	Centro de Datos	2	2	2	2,00
A4	Biométricos	Físico y Lógico	Sala de recepción Institucional	1	1	1	1,00
A5	Cámaras de seguridad	Físico y Digital	Edificio Institucional	1	1	1	1,00
A6	Switch Core Cisco 4700	Físico y Lógico	Centro de Datos	1	1	3	1,67
A7	Switchs de Acceso Cisco 2960	Físico y Lógico	Centro de Datos	1	1	1	1,00
A8	Enlaces de internet	Físico y Lógico	Centro de Datos	1	1	1	1,00
A9	Antivirus Institucional	Lógico	Centro de Datos	1	1	2	1,33
A10	Sistema Talento Humano SIRHA	Lógico	Centro de Datos	1	1	1	1,00

* La valoración del impacto de un activo (VA), es el promedio de los valores de las tres dimensiones de la Gestión de la Seguridad de la Información:

$$VA = \frac{C + I + D}{3}$$

Identificación de Amenazas

Se deben identificar las amenazas y sus orígenes. Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas, por lo tanto, a las organizaciones.

Algunas amenazas pueden afectar a más de un activo. En tales casos pueden causar diferentes impactos dependiendo los activos que se vean afectados.

Ejemplo de análisis de riesgos:

ANÁLISIS DE RIESGOS			
Subprocesos	**Nro. Activo**	**Nombre Activo**	**Amenaza**
Infraestructura	**A1**	Controladora Wireless, puntos de acceso	Intrusos en la red
			Indisponibilidad de servicios
	A2	Red de datos	Indisponibilidad de servicios
	A3	Firewall Fortigate	Acceso no deseado a activos críticos
			Indisponibilidad de servicios
	A4	Biométricos	Desarrollo de nuevas funcionalidades para la gestión de TH
	A5	Cámaras de seguridad	Acceso de personas no deseables y/o pérdidas de activos.
			Acceso de personas no deseables y/o pérdidas de activos.

Identificación de Vulnerabilidades

Se debe identificar las vulnerabilidades que pueden ser explotadas por las amenazas para causar daños a los activos o a la institución.

La sola presencia de una vulnerabilidad no causa daño por sí misma, dado que es necesario que haya una amenaza presente para explotarla. Una vulnerabilidad que no tiene una amenaza correspondiente puede no requerir de la implementación de un control, pero es recomendable reconocerla y monitorearla para determinar los cambios. Conviene anotar que un control implementado de manera incorrecta o que funciona mal, o un control que se utiliza de modo incorrecto podrían por sí solo constituir una vulnerabilidad.

Ejemplo del análisis de riesgos:

ANÁLISIS DE RIESGOS				
Subprocesos	**Nro. Activo**	**Nombre Activo**	**Amenaza**	**Vulnerabilidad**
Infraestructura	A1	Controladora Wireless, puntos de acceso	Intrusos en la red	Actualización de firmware equipo antiguo
			Indisponibilidad de servicios	No existe equipo de redundancia
	A2	Red de datos	Indisponibilidad de servicios	Red de datos mixta (cat. 5e, 6a)
	A3	Firewall Fortigate	Acceso no deseado a activos críticos	imposibilidad de actualizar firmware por falta de recursos del equipo
			Indisponibilidad de servicios	Inexistencia de equipo de redundancia
	A4	Biométricos	Desarrollo de nuevas funcionalidades para la gestión de TH	Incompatibilidad del software base con plataforma de desarrollo actual (php)
	A5	Cámaras de seguridad	Acceso de personas no deseables y/o pérdidas de activos.	Existencia de áreas sin vigilancia
			Acceso de personas no deseables y/o pérdidas de activos.	Vigencia Tecnología, equipos continuamente dañados

Identificación de Existencia de Controles

"Se debe identificar los controles existentes y los planificados".

Se debe realizar la identificación de los controles existentes para evitar trabajo o costos innecesarios, por ejemplo, en la duplicación de los controles. Además, mientras se identifican los controles existentes es recomendable hacer una verificación para garantizar que los controles funcionan correctamente - una referencia a los reportes de auditoría del SGSI ya existente debería limitar el tiempo que tarda esta labor. Si el control no funciona como se espera, puede causar vulnerabilidades.

Ejemplo de los controles existentes (implementados):

ANÁSLIS DE RIESGOS					EVALUACIÓN DE RIESGOS				
					Impacto	Probabilidad		controles implementados existentes	Cálculo de Evaluación Riesgo
Subprocesos	Nro. Activo	Nombre Activo	Amenaza	Vulnerabilidad	CID	Nivel de amenaza	Nivel de vulnerabilidad		
Infraestructura	A4	Controladora Wireless, puntos de acceso	Indisponibilidad de servicios	Red de datos mixta (cat. 5e, 6a)	1,67	1	1	Mantenimiento local	1,67
Infraestructura	A5	Red de datos	Acceso no deseado a activos críticos	imposibilidad de actualizar firware por falta de recursos del equipo	2,00	2	2	Soporte contratado	8,00
			Indisponibilidad de servicios	Inexistencia de equipo de redundancia	2,00	2	2	Soporte contratado	8,00
Infraestructura	A6	Firewall Fortigate	Desarrollo de nuevas funcionalidades para la gestión de TH	Incompatibilidad del software base con plataforma de desarrollo actual (php)	1,00	1	1	Mantenimiento local	1,00
Infraestructura	A7	Biometricos	No cumplimiento de actividades del usuario con daño en su equipo	Ausencia de equipos de reemplazo temporal	1,33	1	2	Mantenimiento local	2,67
			Disminución de la gestión del proceso	Hardware con recursos limitados	1,33	1	2	Mantenimiento local	2,67
Infraestructura	A9	Cámaras de Seguridad	Acceso de personas no deseables y/o pérdidas de activos.	Existencia de áreas sin vigilancia	1,00	1	2	Mantenimiento local	2,00
			Acceso de personas no deseables y/o pérdidas de activos.	Vigencia Tecnología, equipos continuamente dañados	1,00	1	1	Mantenimiento local	1,00

Estimación o Análisis del riesgo

"Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo"

Consiste en utilizar métodos cuantitativos o cualitativos para obtener una cuantificación de los riesgos identificados, tomando en cuenta los activos, las amenazas y las políticas.

Luego de identificar los riesgos, el marco de trabajo debe considerar una metodología de análisis de riesgo. El análisis de riesgo cualitativo usa una escala de calificación de atributos para describir la magnitud de las consecuencias potenciales (por ejemplo, baja, media y alta) y la probabilidad de esas consecuencias.

Evaluación del riesgo

Consiste en comparar los riesgos estimados con los criterios de evaluación y de aceptación de riesgos definidos en el establecimiento del contexto.

Proceso de comparación del riesgo estimado contra un criterio de riesgo calculado dado para determinar la importancia del riesgo. El grado del riesgo es expresado numéricamente basado en las medidas del valor de los activos de información, el impacto de la amenaza y el alcance de la vulnerabilidad.

Criterios de probabilidad de ocurrencia de amenazas:

En la tabla se detallan los criterios calificativos y los valores numéricos a ser utilizados para la valoración de la probabilidad de amenazas que podrían explotar alguna vulnerabilidad existente.

Nivel de amenazas	Criterio por probabilidad	Criterio por condición de ocurrencia	Criterio por atractivo	Ejemplo
Alto (3)	La ocurrencia es muy probable (probabilidad > 50%)	Bajo circunstancias normales	El atacante se beneficia en gran medida por el ataque, tiene la capacidad técnica para ejecutarlo y la vulnerabilidad es fácilmente explotable	Código malicioso
Medio (2)	La ocurrencia es probable	Por errores descuidos	El atacante se beneficia de alguna manera por el ataque,	Falla de hardware

	(probabilidad =50%)		tiene la capacidad técnica para ejecutarlo y la vulnerabilidad es fácilmente explotable	
Bajo (1)	La ocurrencia es menos probable (probabilidad >0 y <50%)	en rara ocasión	El atacante no se beneficia del ataque	desastres naturales

Criterio de probabilidad de ocurrencia de vulnerabilidades

NIVEL DE VULNERABILIDAD	CRITERIO	EJEMPLO
Alto (3)	No existe ninguna medida de seguridad implementada para prevenir la ocurrencia de la amenaza	No se utilizan contraseñas para que los usuarios ingresen a los sistemas
Medio (2)	Existen medidas de seguridad implementadas que no reducen la probabilidad de ocurrencia de la amenaza a un nivel aceptable	Existen normas para la utilización de contraseñas, pero no se implementa
Bajo (1)	La medida de seguridad es adecuada	Existen normas para la utilización de contraseñas y es aplicada

Criterio de la Evaluación de Riesgos

El producto de la probabilidad de ocurrencia de una amenaza, la probabilidad de ocurrencia de vulnerabilidades y el valor del impacto del activo de la información (CID), tenemos como resultado el nivel de riesgo de cada activo

$$\boldsymbol{Nivel\ de\ riesgo} = \mathbf{VA(CID)} * \mathbf{Nivel\ de\ amenaza} * \mathbf{Nivel\ de\ vulnerabilidad}$$

Nivel de Riesgo	
1 - 3	**El riesgo es BAJO**
4 - 8	**El riesgo es MEDIO**
9 - 27	**El riesgo es ALTO**

				Evaluación de Riesgos					
				Impacto	Probabilidad		controles implementados existentes	Cálculo de Evaluación Riesgo	Nivel de Riesgo
Nro. Activo	Nombre Activo	Amenaza	Vulnerabilidad	CID	Nivel de amenaza	Nivel de vulnerabilidad			
A1	Controladora Wireless, puntos de acceso	Intrusos en la red	Actualización de firware equipo antiguo	1,33	1	1	Soporte contratado	1,33	**BAJO**
		Indisponibilidad de servicios	No existe equipo de redundancia	1,33	1	1	Soporte contratado	1,33	**BAJO**
A2	Red de datos	Indisponibilidad de servicios	Red de datos mixta (cat. 5e, 6a)	1,67	1	1	Mantenimiento local	1,67	**BAJO**
A3	Firewall Fortigate	Acceso no deseado a activos críticos	imposibilidad de actualizar firware por falta de recursos del equipo	2,00	2	2	Soporte contratado	8,00	**MEDIO**
		Indisponibilidad de servicios	Inexistencia de equipo de redundancia	2,00	2	2	Soporte contratado	8,00	**MEDIO**
A4	Biometricos	Desarrollo de nuevas funcionalidades para la gestión de TH	Incompatibilidad del software base con plataforma de desarrollo actual (php)	1,00	1	1	Mantenimiento local	1,00	**BAJO**
A5	Cámaras de seguridad	Acceso de personas no deseables y/o pérdidas de activos.	Existencia de áreas sin vigilancia	1,00	1	2	Mantenimiento local	2,00	**BAJO**
		Acceso de personas no deseables y/o pérdidas de activos.	Vigencia Tecnología, equipos continuamente dañados	1,00	1	1	Mantenimiento local	1,00	**BAJO**

Ejemplo del cálculo de la evaluación de riesgos:

TRATAMIENTO DEL RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN

El tratamiento de los riesgos es tomar decisiones frente a los diferentes riesgos existentes de acuerdo a la estrategia de la institución.
Se deben seleccionar controles para reducir, aceptar/retener, evitar o transferir los riesgos y se debe definir un plan para el tratamiento del riesgo.

Existen cuatro opciones disponibles para el tratamiento del riesgo:

- Reducción del riesgo
- Aceptación del riesgo
- Evitación del riesgo
- Transferencia del riesgo

La Figura ilustra la actividad del tratamiento del riesgo dentro de los procesos de gestión del riesgo de la seguridad de la información:

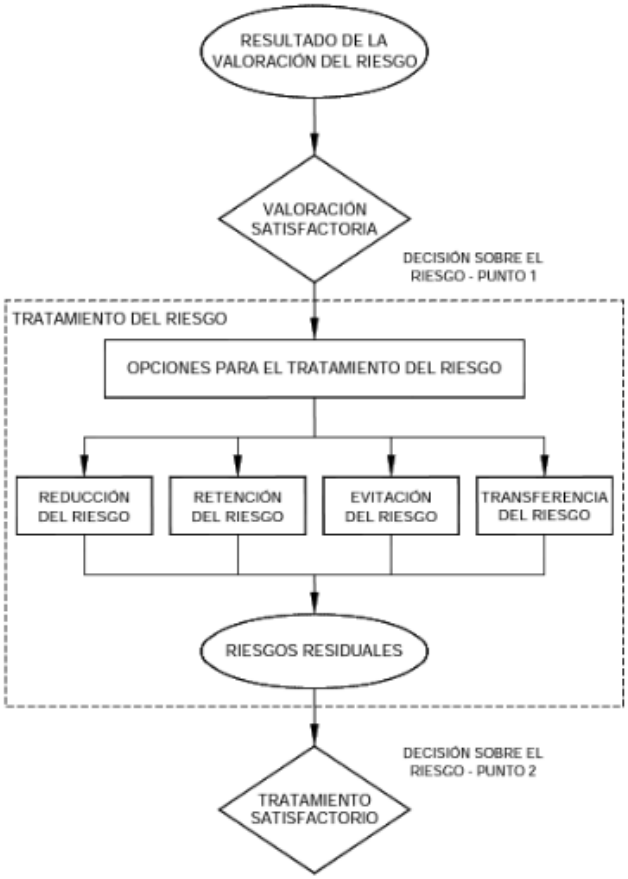

Figura No. 3 ACTIVIDADES PARA EL TRATAMIENTO DE LOS RIESGOS
Fuente: ISO27005

Las opciones para el tratamiento del riesgo se deberían seleccionar con base en el resultado de la valoración del riesgo, el costo esperado para implementar estas opciones y los beneficios esperados como resultado de tales opciones.
Cuando se pueden obtener reducciones grandes en los riesgos con un costo relativamente bajo, se deberían implementar esas opciones. Las opciones adicionales para las mejoras pueden no ser económicas y es necesario estudiarlas para determinar si se justifican o no.

En general, las consecuencias adversas de los riesgos deberían ser tan bajas como sea razonablemente viable e independientemente de cualquier criterio absoluto. En tales casos, puede ser necesario implementar controles que no son justificables en términos estrictamente económicos (por ejemplo, los controles para la continuidad del negocio considerados para cumplir riesgos altos específicos).

Reducción del riesgo

Se debe reducir mediante la selección de controles, de manera tal que el riesgo residual se pueda reevaluar como aceptable.

Se debe seleccionar controles adecuados y justificados que satisfagan los requisitos identificados en la valoración y el tratamiento del riesgo. En esta selección se deberían tener en cuenta los criterios de aceptación del riesgo, así como requisitos legales, reglamentarios y contractuales. En esta selección también se deberían considerar los costos y el tiempo para la implementación de los controles, o los aspectos técnicos, ambientales y culturales. Con frecuencia es posible disminuir el costo total de la propiedad de un sistema con controles de seguridad de la información adecuadamente seleccionados.

"…tiene por objetivo reducir el nivel del riesgo para a su vez reducir el impacto y la probabilidad de ocurrencia de daños sobre los activos de información de la organización…"

Evitación del riesgo

Se debe evitar la actividad o la acción que da origen al riesgo particular.

Cuando los riesgos identificados se consideran muy altos, o si los costos para implementar otras opciones de tratamiento del riesgo exceden los beneficios, se puede tomar una decisión para evitar por completo el riesgo, mediante el retiro de una actividad o un conjunto de actividades planificadas o existentes, o mediante el cambio en las condiciones bajo las cuales se efectúa tal actividad.

Por ejemplo, para los riesgos causados por la naturaleza, puede ser una alternativa más eficaz en términos de costo, transferir físicamente las instalaciones de procesamiento de la información a un lugar donde no exista el riesgo o esté bajo control

Transferencia del riesgo

El riesgo se debe transferir a otra parte que pueda gestionar de manera más eficaz el riesgo particular dependiendo de la evaluación del riesgo.

Retención/aceptación del riesgo

La decisión sobre la retención del riesgo sin acción posterior se debería tomar dependiendo de la evaluación del riesgo.

Aceptar los riesgos con conocimiento y objetividad, siempre y cuando satisfagan claramente la política y los criterios de la institución para la aceptación de los riesgos.

Ejemplo del tratamiento de los riesgos:

Evaluación de Riesgos						Tratamiento de Riesgos							
Impacto	Probabilidad		controles implementados existentes	Cálculo de Evaluación Riesgo	Nivel de Riesgo	Método de tratamiento de Riesgos	Tipo de control	Controles a Implementar	Nivel de amenaza	Nivel de vulnerabilidad	Cálculo de Evaluación Riesgo con el control implementado	Nivel de Riesgo con el control Implementado	Riesgo residual
CID	Nivel de amenaza	Nivel de vulnerabilidad											
1,67	2	2	Soporte contratado	6,67	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	Migración a Cloud	1	1	1,67	BAJO	ACEPTABLE
1,67	2	2	Plan aplicado de pruebas y backup	6,67	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	Migración a Cloud	1	1	1,67	BAJO	ACEPTABLE
1,67	2	2	Plan aplicado de pruebas y backup	6,67	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	Migración a Cloud	1	1	1,67	BAJO	ACEPTABLE
1,67	1	2	Soporte contratado	3,33	BAJO	ACEPTAR	CONTROL PREVENTIVO	Migración a Cloud	1	1	1,67	BAJO	ACEPTABLE
1,67	2	2	Soporte contratado	6,67	MEDIO	MITIGAR / EVITAR / TRANSFERIR	CONTROL PREVENTIVO	Migración a Cloud	1	1	1,67	BAJO	ACEPTABLE
1,67	1	2	Soporte contratado	3,33	BAJO	ACEPTAR	CONTROL PREVENTIVO	Migración a Cloud	1	1	1,67	BAJO	ACEPTABLE

ACEPTACIÓN DEL RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN

Se deber tomar la decisión de aceptar los riesgos y las responsabilidades de la decisión, y registrarla de manera formal.

Esta opción se toma cuando los costos de implementación de un control de seguridad sobrepasan el valor del activo de información que se desea proteger o cuando el nivel del riesgo es muy bajo, en ambos casos la organización asume los daños provocados por la materialización del riesgo.

En algunos casos, es posible que el nivel del riesgo residual no satisfaga los criterios de aceptación del riesgo porque los criterios que se aplican no toman en consideración las circunstancias prevalentes. Por ejemplo, se puede argumentar que es necesario aceptar los riesgos porque los beneficios que los acompañan son muy atractivos o porque el costo de la reducción del riesgo es demasiado alto.

La organización debería definir sus propias escalas para los niveles de aceptación del riesgo.

Durante el desarrollo, se deberían considerar los siguientes aspectos:

- *Los criterios de aceptación del riesgo pueden incluir umbrales múltiples*, con una meta de nivel de riesgo deseable, pero con disposiciones para que la alta dirección acepte los riesgos por encima de este nivel, en circunstancias definidas.
- Los criterios de aceptación del riesgo se pueden expresar como la relación entre el beneficio estimado (u otros beneficios del negocio) y el riesgo estimado.
- Los diferentes criterios de aceptación del riesgo se pueden aplicar a diferentes clases de riesgos, por ejemplo, los riesgos que podrían resultar en incumplimiento con reglamentos o leyes, podrían no ser aceptados, aunque se puede permitir la aceptación de riesgos altos, si esto se especifica como un requisito contractual.

- Los criterios de aceptación del riesgo pueden incluir requisitos para tratamiento adicional en el futuro, por ejemplo, se puede aceptar un riesgo si existe aprobación y compromiso para ejecutar acciones que reduzcan dicho riesgo hasta un nivel aceptable en un periodo definido de tiempo.

COMUNICACIÓN DE LOS RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN

"La información acerca de los riesgos se debe intercambiar y/o compartir entre quienes toman las decisiones y las partes involucradas."

La comunicación del riesgo es una actividad para lograr un acuerdo sobre la manera de gestionar los riesgos al intercambiar y/o compartir la información acerca de los riesgos. La información incluye, pero no se limita a la existencia, naturaleza, forma, probabilidad, gravedad, tratamiento y aceptabilidad de los riesgos.

La comunicación eficaz entre las partes involucradas es importante dado que puede tener un impacto significativo en las decisiones que se deben tomar. La comunicación garantizará que aquellos responsables de la implementación de la gestión del riesgo y aquellos con intereses establecidos comprendan las bases sobre las cuales toman las decisiones y por qué se requieren acciones particulares. La comunicación es bidireccional.

La comunicación del riesgo se debería realizar con el fin de lograr lo siguiente:

- Proporcionar seguridad del resultado de la gestión del riesgo de la institución.
- Recolectar información del riesgo.
- Compartir los resultados de la valoración del riesgo y presentar el plan para el tratamiento del riesgo.
- Evitar o reducir tanto la ocurrencia como la consecuencia de las brechas de seguridad de la información debido a la falta de entendimiento entre quienes toman las decisiones y las partes involucradas.
- Brindar soporte para la toma de decisiones.

- Obtener conocimientos nuevos sobre la seguridad de la información.
- Coordinar con otras partes y planificar las respuestas para reducir las consecuencias de cualquier incidente.
- Dar a quienes toman las decisiones y a las partes involucradas un sentido de responsabilidad acerca de los riesgos.
- Mejorar la toma de conciencia.

La coordinación entre las personas principales que toman las decisiones y las partes involucradas se puede lograr en el Comité de Seguridad de la Información (CSI) en el cual pueda tener lugar el debate acerca de los riesgos, su prioridad, el tratamiento adecuado y la aceptación.

MONITOREO Y REVISIÓN DEL RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN

Monitoreo y revisión de los factores de riesgo

Los riesgos no son estáticos. Las amenazas, las vulnerabilidades, la probabilidad o las consecuencias pueden cambiar abruptamente sin ninguna indicación. Por ende, es necesario el monitoreo constante para detectar estos cambios.

Esta actividad puede estar soportada por servicios externos que brinden información con respecto a nuevas amenazas o vulnerabilidades.

Las organizaciones deberían garantizar el monitoreo continuo de los siguientes aspectos:

- Activos nuevos que se han incluido en el alcance de la gestión del riesgo.
- Modificaciones necesarias de los valores de los activos, por ejemplo, debido a cambios en los requisitos del negocio.
- Nuevas amenazas que podrían estar activas tanto fuera como dentro de la organización y que no se han valorado.
- Probabilidad de que nuevas vulnerabilidades o el incremento en las vulnerabilidades existentes permitan que las amenazas las exploten.

- Vulnerabilidades identificadas para determinar aquellas que se exponen a nuevas amenazas o que vuelven a surgir.
- El incremento en el impacto o las consecuencias de las amenazas evaluadas, las vulnerabilidades y los riesgos en conjunto que dan como resultado un nivel inaceptable de riesgo.
- Incidentes de la seguridad de la información.

Los factores que afectan a la probabilidad y a las consecuencias de las amenazas que se presentan podrían cambiar, como lo harían los factores que afectan a la idoneidad o el costo de las diversas opciones de tratamiento. Los cambios importantes que afectan a la organización deberían ser la razón para una revisión más específica. Por lo tanto, las actividades de monitoreo del riesgo se deberían repetir con regularidad y las opciones seleccionadas para el tratamiento del riesgo se deberían revisar periódicamente.

Monitoreo, revisión y mejora de la gestión del riesgo

"El proceso de gestión del riesgo en la seguridad de la información se debe monitorear, revisar y mejorar continuamente, según sea necesario y adecuado".

El monitoreo y la revisión continuos son necesarios para garantizar que el contexto, el resultado de la valoración del riesgo y el tratamiento del riesgo, así como los planes de gestión siguen siendo pertinentes y adecuados para las circunstancias actuales.

La organización debe garantizar que el proceso de gestión del riesgo de la seguridad de la información y las actividades relacionadas aún son adecuadas en las circunstancias actuales y se cumplen. Todas las mejoras acordadas para el proceso o las acciones necesarias para mejorar la conformidad con el proceso se deberían notificar al Comité de Seguridad de la Información, para tener seguridad de que no se omite ni subestima ningún riesgo o elemento del riesgo, y que se toman las acciones necesarias y las decisiones para brindar una comprensión realista del riesgo y la capacidad para responder.

GLOSARIO DE TÉRMINOS

Lista de términos relacionados en el contexto del Esquema Gubernamental de la Seguridad de la Información:

A.

Activo de información. - En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la institución.

Amenaza. - causa potencial de un incidente no deseado, que puede resultar en un daño a un sistema, persona u organización.

Análisis de riesgos. - proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Aplicación. – solución de TI, incluyendo programas de aplicación, datos de aplicaciones y procedimientos diseñados para ayudar a los usuarios de las organizaciones a realizar tareas específicas o manejar tipos específicos de problemas de TI, automatizando un proceso o función del negocio

Ataque. - intento de destruir, exponer, alterar, deshabilitar, robar o lograr acceso no autorizado o hacer uso no autorizado de un activo.

Autenticación. - Provisión de una garantía de que una característica afirmada por una entidad es correcta.

Autenticidad. - Propiedad de que una entidad es lo que afirma ser.

C.

Comité de Seguridad de la información (CSI). – se encarga de gestionar la implementación y mejora continua del Esquema Gubernamental de Seguridad de la Información.

Confidencialidad. - Propiedad de que la información no esté disponible o no sea divulgada a personas, entidades o procesos no autorizados.

Contenidos maliciosos. - Aplicaciones, documentos, archivos, datos u otros recursos que tienen características o capacidades maliciosas incrustadas, disfrazadas o escondidas en ellos.

Control. - Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Control contramedida. - los medios de gestión de riesgos, que incluyen las políticas, procedimientos, directrices, prácticas o estructuras organizativas, que pueden ser de carácter administrativo, técnico, de gestión o de carácter legal.

D.

Directiva o directriz. - Una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

Disponibilidad. - Propiedad de estar disponible y utilizable en el momento que sea requerido por una entidad autorizada.

E.

EGSI. - Esquema Gubernamental de Seguridad de la Información para las instituciones de la APCID para preservar la integridad, disponibilidad y confidencialidad de la información.

Evaluación de riesgos. - Proceso global de identificación, análisis y estimación de riesgos.

G.

Gestión de claves. - Controles referidos a la gestión de claves criptográficas.

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

Gestión de riesgos. - Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

I.

Identificación de riesgos. - Proceso de encontrar, reconocer y describir riesgos.

Impacto. - El costo para la institución de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros (ejem.: pérdida de reputación, implicaciones legales, entre otros).

Incidente de seguridad de la información. - Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Información.- Es uno de los activos más importantes de las instituciones, en las formas que esta se manifieste: textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, magnético, papel, electrónico, computadoras, audiovisual y otros.

Institución. - Grupo de personas e instalaciones con una disposición de responsabilidades, autoridades y relaciones.

Integridad. - Propiedad de proteger la precisión y completitud de los activos.

Internet (red interconectada), interconexión de redes. - una colección de redes interconectadas.
“La internet. - sistema global de redes interconectadas de dominio público”

Inventario de activos. - Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.)

dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

N.

No repudio. - Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).

M.

Malware, software malicioso. - Software diseñado con malas intenciones que contiene características o capacidades que potencialmente pueden causar daño directamente o indirectamente al usuario y/o al sistema informático del usuario.

O.

Objetivo. - Declaración del resultado o fin que se desea lograr mediante la implementación de procedimientos de control en una actividad determinada.

Oficial de Seguridad de la Información (OSI). - Es el responsable de coordinar las acciones del Comité de Seguridad de la Información y de impulsar la implementación y cumplimiento del Esquema

P.

Parte interesada. - <gestión de riesgos> persona u organización que puede afectar, verse afectada por, o percibirse a sí misma como afectada por una decisión o actividad.

Phishing (engaño técnico). - proceso fraudulento o intento de adquirir información privada o confidencial de manera enmascarada haciéndose pasar por una entidad confiable en una comunicación electrónica.

Plan de continuidad del negocio. - Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.

Plan de tratamiento de riesgos. - Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Política de escritorio despejado. - La política de la empresa que indica a los empleados que deben dejar su área de trabajo libre de cualquier tipo de informaciones susceptibles de mal uso en su ausencia.

Proceso. - Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.

Propietario del activo. - puede no tener derechos de propiedad sobre el activo, pero tiene la responsabilidad de su producción, desarrollo, mantenimiento, uso y seguridad, según corresponda. El propietario del activo con frecuencia es la persona más idónea para determinar el valor que el activo tiene para la institución.

Propietario de la Información. - es el responsable de clasificar la información de acuerdo con el grado de sensibilidad y criticidad de la misma, de documentar y mantener actualizada la clasificación efectuada y de definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia.

Propietario del riesgo. - persona o entidad con responsabilidad y autoridad para gestionar un riesgo.

Proveedor de servicios de Internet. - organización que presta servicios de Internet a un usuario y permite a sus clientes acceder a Internet.

R.

Resiliencia. - Capacidad de los activos institucionales, para regresar a su forma original.

Riesgo. - Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

Riesgo residual. - El riesgo que permanece tras el tratamiento del riesgo.

S.

Seguridad de la información. - conjunto de medidas preventivas y reactivas de las instituciones y de los sistemas tecnológicos que permiten la preservación de la confidencialidad, integridad y disponibilidad de la información.

Sistema de información. - Aparato o grupo de aparatos interconectados o relacionados entre sí, uno o varios de los cuales realizan, mediante un programa, el tratamiento automático de datos informáticos, así como los datos informáticos almacenados, tratados, recuperados o transmitidos por estos últimos para su funcionamiento, utilización, protección y mantenimiento

Software engañoso (spyware). - que recopila información privada o confidencial de un usuario de computador.

Software potencialmente no deseado. - software engañoso, incluyendo el malware y no malicioso, que exhibe las características de software engañoso.

Spam (correo basura). - abuso de los sistemas de mensajería electrónica para enviar indiscriminadamente mensajes masivos no solicitados.

T.

Tratamiento de riesgos. - Proceso de modificar el riesgo, mediante la implementación de controles.

Trazabilidad. - Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

Troyano, caballo de Troya. - software malintencionado que aparece para realizar una función deseable.

V.

Vulnerabilidad. - Debilidad de un activo o control que puede ser explotada por una o más amenazas.

Dirección Nacional - Interoperabilidad, Seguridad de la Información e Infraestructura

2020-Subsecretaría de Estado-Gobierno Electrónico

www.gobiernoelectronico.gob.ec